

DEFINABILITY AND FAST QUANTIFIER ELIMINATION
IN ALGEBRAICALLY CLOSED FIELDS

Inaugural-Dissertation
zur Erlangung der philosophischen Doktorwürde
vorgelegt der
Philosophischen Fakultät II
der Universität Zürich

von
JOOS HEINTZ
aus Davos GR

Begutachtet von Herrn Prof. Dr. V. Strassen
Zürich 1982



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41507223_0022

Definability and fast quantifier elimination
in algebraically closed fields

Inaugural - Dissertation
zur Erlangung der philosophischen Doktorwürde
vorgelegt der
Philosophischen Fakultät II
der Universität Zürich

von

Joos Heintz

aus Davos GR

Begutachtet von Herrn Prof. Dr. V. Strassen

Zürich 1982



Introduction

This work is a somewhat extended version of (Heintz-Wüthrich 1975), (Heintz 1977), and (Heintz 1979). The paper deals with quantifier elimination in algebraically closed fields (part III)* and related definability problems from the point of view of complexity (part II).

(Fischer - Rabin 1974) have shown that any decision procedure for the theory of algebraically closed fields of given characteristic is exponentially slow in the size of the input formula on some infinite set of formulas. The following adaptation of one aspect of their method shows that any quantifier elimination procedure needs space - and hence time - even double exponential on infinitely many formulas :

Let k be an algebraically closed field, and let $d > 1$ not be divisible by the characteristic of k . For each $\ell = 1, 2, \dots$ we define inductively a first order formula $\phi_\ell(X_1, X_2)$ in the language with "=" and "exponentiation by d " as the only nonlogical symbols, X_1, X_2 being variables.

Let $\phi_1(X_1, X_2)$ be $X_1^d = X_2$.

For given $\phi_\ell(X_1, X_2)$ choose variables Y, Z_1, Z_2 different from X_1, X_2 , such that Z_1 is free for X_1 and Z_2 is free for X_2 in $\phi_\ell(X_1, X_2)$.

Let $\phi_{\ell+1}(X_1, X_2)$ be

$$(\exists Y)(\forall Z_1)(\forall Z_2) (((Z_1 = Y \wedge Z_2 = X_2) \vee (Z_1 = X_1 \wedge Z_2 = Y)) \rightarrow \phi_\ell(Z_1, Z_2)) .$$

Proceeding economically, the formulas $\phi_1(X_1, X_2), \dots, \phi_\ell(X_1, X_2), \dots$ can be defined using seven variables only, as one sees immediately. So we can code $\phi_1(X_1, X_2), \dots, \phi_\ell(X_1, X_2), \dots$ on a Turing-Machine tape such that the length of the $\phi_\ell(X_1, X_2)$ depends only linearly on ℓ .

$\phi_\ell(X_1, X_2)$ defines the graph of the map $\varphi_\ell : k \rightarrow k$ with $\varphi_\ell(x) = x^{d^{2^\ell}}$ for $x \in k$. We have $\#(\varphi_\ell)^{-1}(1) = d^{2^\ell}$ (where $\#$ is the cardinality symbol).

Hence the subset of k defined by $\phi_\ell(X_1, 1)$ contains d^{2^ℓ} elements.

So we have constructed a sequence of formulas (namely $\phi_1(X_1, 1), \dots, \phi_\ell(X_1, 1), \dots$) such that the length of these formulas depends linearly on ℓ and such that the ℓ -th formula defines a subset of k of cardinality d^{2^ℓ} . As it can easily be seen, any quantifier free description of such a set needs space $O(d^{2^\ell})$ on a Turing-Machine tape, a standard encoding of the language of k assumed. Thus quantifier elimination in k needs space double exponential in the length of the input formulas $\phi_1(X_1, 1), \dots, \phi_\ell(X_1, 1), \dots$.

* Part III was done working together with H.R. Wüthrich, Zürich. See also (Wüthrich 1977).

In part III of this paper we show that conversely for algebraically closed fields of any characteristic there exists a quantifier elimination method which runs in time double exponential in the size of the input formula. More precisely, our time bound is polynomial in degree and maximum length of the coefficients of the polynomials appearing in the input formula but double exponential in the number of variables of the input formula. A similar result for real closed fields has previously been obtained by (Collins 1975). (See also (Monck 1974, (Solovay 1975 and (Wüthrich 1976)). Of course, their result implies ours in the case of characteristic zero. However their proofs do not extend to the case of prime characteristic. We remark that, although a double exponential time bound excludes practical applicability in general, several of the ideas involved in our algorithm seem to be of practical significance in special situations. However, important decision problems, although they can be reduced to quantifier elimination of algebraically closed fields, become much more tractable from the point of view of complexity using methods less general than quantifier elimination. (Compare (Heintz-Sieveking 1981)).

Closely related to fast quantifier elimination are questions of the following type: How large can a finite set be which is defined by a formula built up from a given set of polynomials? How many sets (finite or not) can be defined by a given set of polynomials using logical connectives (including quantifiers)?

Part II deals with questions of this kind. It turns out that the decisive parameters to answer these questions are the sum of the degrees of the polynomials, the total number of variables, and the number of bounded variables appearing in the formulas under consideration.

Our methods are based on some elementary affine algebraic geometry. Particularly useful is a version of Bezout's Theorem without multiplicities which we call the Bezout-Inequality. Although we have little information about multiplicities, the Bezout-Inequality has the advantage that it holds without any restriction on the kind of the intersection. Moreover it allows a relatively elementary proof, which we give in part I, since the Bezout-Inequality has many applications to algebraic complexity theory. (See (Strassen 1973), where the Bezout Theorem in its classical form is used, (Heintz 1977), (Heintz 1979), (Heintz-Schnorr 1980), (Heintz-Sieveking 1980), (Schnorr 1981), (Strassen 1981), (Baur-Strassen 1981).)

I. The Bezout Inequality

In this part we introduce the notion of degree first for irreducible closed and then for arbitrary constructible subsets of affine spaces and prove the Bezout - Inequality.

We need some prerequisites from classical algebraic geometry and commutative algebra, which can be found in (Mumford), Chapter I, or in (Shafarevich 1972), Chapter I, and, as concerning commutative algebra, in (Atiyah - Macdonald 1969).

We use the same terminology as these authors.

For field theory we refer to (van der Waerden 1971 and Lang 1969).

The notion and elementary properties of degree of irreducible closed subsets of affine spaces are based on the following proposition.

By lack of direct references to quote here, we give a proof of it, elementary in the sense that only dimension theory is used.

Proposition 1: Let W be an affine variety of dimension m and $\varphi : W \rightarrow \mathbb{A}^m$ a dominating morphism (i.e. with $\overline{\varphi(W)} = \mathbb{A}^m$), where $\mathbb{A}^m$ denotes the affine space of dimension m . The field extension $k(\mathbb{A}^m) \subset k(W)$ induced by φ is finite. Assume it to be separable.

Then

- (i) $\# \varphi^{-1}(y) \leq [k(W) : k(\mathbb{A}^m)]$ for $y \in \mathbb{A}^m$ with finite fibre $\varphi^{-1}(y)$.
- (ii) There is a nonempty open $U \subset \mathbb{A}^m$ so that equality holds in (i) for $y \in U$.

Proof: Assertion (i), the harder to prove, follows easily from (Shafarevich 1972), Chapter II, § 6, Theorem 6, and Zariski's Main Theorem (Iversen 1973). Here we give an elementary proof avoiding Zariski's Main Theorem.

We show (i) by induction on m , dropping the assumption on separability of the field extension $k(\mathbb{A}^m) \subset k(W)$.

The case $m=0$ is obvious.

So, let $m > 0$ and $y = (y_1, \dots, y_m) \in \mathbb{A}^m$ with finite fibre.

We identify $\mathbb{A}^{m-1}$ with the hyperplane $\mathbb{A}^{m-1} \times \{y_m\}$ of $\mathbb{A}^m$.

This hyperplane $\mathbb{A}^{m-1}$ contains y . Furthermore, $\varphi^{-1}(\mathbb{A}^{m-1})$ is a hypersurface of W containing $\varphi^{-1}(y)$. Hence, by the Dimension Theorem (Shafarevich 1972), Chapter I, § 6, Corollary 1 of Theorem 5 or (Mumford), Chapter I, § 7, Theorem 2, all components of $\varphi^{-1}(\mathbb{A}^{m-1})$ have dimension $m-1$.

Let C be a component of $\varphi^{-1}(\mathbb{A}^{m-1})$. We have $\dim C = m-1$ and $\varphi(C) \subset \mathbb{A}^{m-1}$.

We consider the morphism $\varphi_C : C \rightarrow \overline{\varphi(C)}$ induced by φ on C .

If $\overline{\varphi(C)} = \mathbb{A}^{m-1}$ we can apply the induction hypothesis on φ_C . So we have $\# \varphi^{-1}(y) \cap C = \# \varphi_C^{-1}(y) \leq [k(C) : k(\mathbb{A}^{m-1})]$ in this case.

If $\overline{\varphi(C)} \neq \mathbb{A}^{m-1}$ we have $\dim \overline{\varphi(C)} < m-1 = \dim C$.

By the theorem of fibres of a morphism (Mumford), Chapter I, § 8, Theorem 2 or (Shafarevich 1972), Chapter I, § 6, Theorem 7, the components of the φ_C -fibres of points of $\overline{\varphi(C)}$ have dimension $\geq \dim C - \dim \overline{\varphi(C)} > 0$.

Therefore the φ -fibres of points of $\varphi(C)$ are infinite. Since $\varphi^{-1}(y)$ is finite, we have $\varphi^{-1}(y) \cap C = \emptyset$ in this case.

Let $c := \{C; C \text{ is a component of } \varphi^{-1}(\mathbb{A}^{m-1}) \text{ with } \overline{\varphi(C)} = \mathbb{A}^{m-1}\}$. We have shown $\varphi^{-1}(y) = \bigcup_{C \in c} \varphi^{-1}(y) \cap C$ and $\# \varphi^{-1}(y) \leq [k(C) : k(\mathbb{A}^{m-1})]$ for $C \in c$.

So we have $\# \varphi^{-1}(y) \leq \sum_{C \in c} [k(C) : k(\mathbb{A}^{m-1})]$.

To finish the proof of (i), it suffices to show

$$\sum_{C \in c} [k(C) : k(\mathbb{A}^{m-1})] \leq [k(W) : k(\mathbb{A}^m)].$$

Let $C \in \mathcal{C}$. The diagram of affine varieties

$$\begin{array}{ccc} \mathbb{A}^m & \longleftarrow & W \\ \cup & & \cup \\ \mathbb{A}^{m-1} & \longleftarrow & C \end{array}$$

induces a diagram of coordinate rings

$$\begin{array}{ccc} k[\mathbb{A}^m] & \longrightarrow & k[W] \\ \downarrow & & \downarrow \\ k[\mathbb{A}^{m-1}] & \longrightarrow & k[C] \end{array}$$

in which the top and the bottom morphisms are injective. (The injectivity follows from the fact that $W \rightarrow \mathbb{A}^m$ and $C \rightarrow \mathbb{A}^{m-1}$ are dominating morphisms.)

Let $P := \{\sigma; \sigma \in k[\mathbb{A}^m], \sigma \text{ doesn't vanish identically on } \mathbb{A}^{m-1}\}$.

To simplify notations, we also write P for its images in the rings $k[\mathbb{A}^{m-1}]$, $k[W]$, and $k[C]$.

P is in $k[\mathbb{A}^m]$ the complement of the prime ideal of functions of $k[\mathbb{A}^m]$ vanishing at every point of $\mathbb{A}^{m-1}$. So it can easily be seen that P is in any of the rings $k[\mathbb{A}^m]$, $k[\mathbb{A}^{m-1}]$, $k[W]$, $k[C]$ a multiplicative closed set with $1 \in P$ which doesn't contain zero. Hence the localizations of these rings by P can be embedded in their corresponding fields of fractions.

The field extension $k(\mathbb{A}^{m-1}) \subset k(C)$ induced by the dominating morphism $C \rightarrow \mathbb{A}^{m-1}$ is finite. So $k(C)$ is a finite dimensional $k(\mathbb{A}^{m-1})$ -algebra.

The same morphism induces a ring homomorphism $P^{-1}k[\mathbb{A}^{m-1}] \rightarrow P^{-1}k[C]$.

Note $P^{-1}k[\mathbb{A}^{m-1}] = k(\mathbb{A}^{m-1})$. So $P^{-1}k[C]$ is a $k(\mathbb{A}^{m-1})$ -subalgebra of $k(C)$ and hence finite dimensional over $k(\mathbb{A}^{m-1})$.

Any finite dimensional $k(\mathbb{A}^{m-1})$ -algebra without zero divisors is a field.

(This follows from (Atiyah-Macdonald 1969), Chapter 8, Ex. 3 and Prop. 8.1.)

So $P^{-1}k[C]$ is a subfield of $k(C)$ containing $k[C]$, whence $P^{-1}k[C] = k(C)$.

The inclusion map $C \subset W$ induces a surjective ring homomorphism $P^{-1}k[W] \rightarrow P^{-1}k[C] = k(C)$. Since its image is a field, its kernel must be a maximal ideal of $P^{-1}k[W]$.

C has been chosen arbitrary from $\mathcal{C}$. Hence we have the same situation for each $C \in \mathcal{C}$. So, by the Chinese Remainder Theorem ((Atiyah-Macdonald 1969), Prop. 1.10 (ii)), we obtain a surjective homomorphism $f: P^{-1}k[W] \rightarrow \bigoplus_{C \in \mathcal{C}} k(C)$ from the $P^{-1}k[A^m]$ -algebra $P^{-1}k[W]$ onto the $k(A^{m-1})$ -algebra $\bigoplus_{C \in \mathcal{C}} k(C)$.

It suffices to show that f maps elements of $P^{-1}k[W]$ which are linearly dependent over $P^{-1}k[A^m]$ on elements of $\bigoplus_{C \in \mathcal{C}} k(C)$ which are linearly dependent over $k(A^{m-1})$.

For then, we can choose in each $k(C)$, $C \in \mathcal{C}$, a $k(A^{m-1})$ -basis E_C .

The union $E = \bigcup_{C \in \mathcal{C}} E_C$ of all these bases is a $k(A^{m-1})$ -linearly independent subset of $\bigoplus_{C \in \mathcal{C}} k(C)$ with $\sum_{C \in \mathcal{C}} [k(C) : k(A^{m-1})]$ elements.

We pick $\sum_{C \in \mathcal{C}} [k(C) : k(A^{m-1})]$ elements of $P^{-1}k[W]$, forming a set $F \subset P^{-1}k[W]$, which is mapped by f on E . (This is possible since f is surjective.) F is a $P^{-1}k[A^m]$ -linearly independent set, for otherwise, f would map F on a $k(A^{m-1})$ -linearly dependent subset of $\bigoplus_{C \in \mathcal{C}} k(C)$, which is impossible, since f maps F one-to-one on E , and E is $k(A^{m-1})$ -linearly independent.

Any $P^{-1}k[A^m]$ -linearly independent subset of $P^{-1}k[W]$ has at most $[k(W) : k(A^m)]$ elements. So we have

$$\sum_{C \in \mathcal{C}} [k(C) : k(A^{m-1})] = \#F \leq [k(W) : k(A^m)].$$

Now we are going to show that the homomorphism $f: P^{-1}k[W] \rightarrow \bigoplus_{C \in \mathcal{C}} k(C)$ maps elements of $P^{-1}k[W]$ which are linearly dependent over $P^{-1}k[A^m]$ on elements of $\bigoplus_{C \in \mathcal{C}} k(C)$ which are linearly dependent over $k(A^{m-1})$.

First note that $P^{-1}k[\mathbb{A}^m]$ is a local ring with a principal maximal ideal (α) with $\alpha \in P^{-1}k[\mathbb{A}^m]$. (This follows from the fact that $P^{-1}k[\mathbb{A}^m] = k[\mathbb{A}^m]_p$, where p is the principal prime ideal of functions of $k[\mathbb{A}^m]$ vanishing on the hyperplane $\mathbb{A}^{m-1}$ of $\mathbb{A}^m$.)

Let $\sigma_1, \dots, \sigma_s \in P^{-1}k[W]$ be linearly dependent over $P^{-1}k[\mathbb{A}^m]$ with $\alpha_1\sigma_1 + \dots + \alpha_s\sigma_s = 0$, $\alpha_1, \dots, \alpha_s \in P^{-1}k[\mathbb{A}^m]$ not all zero. After dividing the $\alpha_1, \dots, \alpha_s$ in the equation $\alpha_1\sigma_1 + \dots + \alpha_s\sigma_s = 0$ by a suitable power of α , we may assume that not all of the $\alpha_1, \dots, \alpha_s$ are divisible by α in $P^{-1}k[\mathbb{A}^m]$.

So let α_1 be not divisible by α . Then we have $\alpha_1 \notin (\alpha)$, i.e. α_1 is a unit of $P^{-1}k[\mathbb{A}^m]$. Consequently we have $f(\alpha_1) \neq 0$ in $k(\mathbb{A}^{m-1})$, $f(\alpha_1) \cdot f(\sigma_1) + \dots + f(\alpha_s) \cdot f(\sigma_s) = 0$. Since $f(\alpha_1), \dots, f(\alpha_s)$ are in $k(\mathbb{A}^{m-1})$, the $f(\sigma_1), \dots, f(\sigma_s)$ are linearly dependent over $k(\mathbb{A}^{m-1})$. This finishes the proof of (i).

(ii) We choose $U \subset \mathbb{A}^m$ open affine such that each element of $k[W]$ is integral over $k[U]$. Furthermore we choose $\sigma \in k[W]$ such that $k[W] \subset k[U][\sigma]$ and such that the discriminant of σ over $k(U)$ is a unit of $k[U]$. (By (van der Waerden 1966), § 46, this is possible since the field extension $k(\mathbb{A}^m) \subset k(W)$ is separable algebraic.)

Without loss of generality we may assume $U = \mathbb{A}^m_g$ for some $g \in k[\mathbb{A}^m]$. So $k[W_g] = k[W]_g = k[U][\sigma]$. We have $W_g = \varphi^{-1}(U)$.

Let S be an indeterminate over $k(U)$. Since $k[U]$ is normal (i.e. integrally closed in $k(U)$), the minimal polynomial $G(S)$ of σ over $k(U)$ is in $k[U][S]$ (Atiyah-Macdonald 1969, prop. 5.15).

Let $G = S^d + a_{d-1} S^{d-1} + \dots + a_0$, $a_{d-1}, \dots, a_0 \in k[U]$,

$$d = [k(U)(\sigma) : k(U)] = [k(W) : k(\mathbb{A}^m)] .$$

To each point $u \in U$ there corresponds a k -algebra homomorphism

$\psi_u : k[U] \rightarrow k$ and to each k -algebra homomorphism $\psi : k[U][\sigma] \rightarrow k$ extending

ψ_u there corresponds a point $w \in W$ with $\varphi(w) = u$. Furthermore the k -algebra

homomorphisms $\psi : k[U][\sigma] \rightarrow k$ extending ψ_u correspond to the zeroes of

$$\psi_u(G) := S^d + \psi_u(a_{d-1}) S^{d-1} + \dots + \psi_u(a_0) .$$

Since by assumption on U , the discriminant of $\psi_u(G)$ doesn't vanish, $\psi_u(G)$ has exactly d distinct zeroes, so we have $\# \varphi^{-1}(u) = d = [k(W) : k(\mathbb{A}^m)]$, whence (ii).

It is worthwhile to note that Proposition 1 remains true if we drop the assumption of separability, but replace in its statement "field degree" by "separability degree".

Furthermore, in Proposition 1 $\mathbb{A}^m$ can be replaced by any smooth affine variety. The proof then runs in a completely analogous way using the fact that the local ring of smooth points are factorial (Shafarevich 1972), Chapter II, § 3, Theorem 2.

The second part of the proof of (i) of Proposition 1 becomes essentially shorter using some elementary valuation theory (compare (Lang 1969), Chapter XII, §§ 4, 5, 6 and (Atiyah-Macdonald 1969), Chapter 5) and the fact that W is a variety. (The property of W to be a variety can be formulated in valuation theoretic terms, namely: local rings of different subvarieties of W cannot be extended to the same valuation ring of $k(W)$, compare (Mumford), Chapter I, § 6 and Chapter II, § 6.). To see this observe that

$P^{-1}k[\mathbb{A}^m]$ is the valuation ring of a discrete valuation v of $k(\mathbb{A}^m)$ with residue class field $k(\mathbb{A}^{m-1})$. Each $k(C)$, $C \in \mathcal{C}$, is contained in some residue class field of some valuation extending v on $k(W)$. To different $C \in \mathcal{C}$ belong different valuation rings of $k(W)$ since W is a variety. But by (Lang 1969), Chapter XII, § 6, Corollary 2, the sum of the degrees of the residue class fields of the valuations extending v on $k(W)$ is bounded by $[k(W) : k(\mathbb{A}^m)]$. So we finally have $\sum_{C \in \mathcal{C}} [k(C) : k(\mathbb{A}^{m-1})] \leq [k(W) : k(\mathbb{A}^m)]$.

We proceed to define the notion of degree by applying Proposition 1 in the following situation:

Let V be a closed subvariety of $\mathbb{A}^n$ with $\dim V = r$.

We associate to V the following morphism $\varphi: \mathbb{A}^m \times V \longrightarrow \mathbb{A}^m \times \mathbb{A}^r$:

we read $\mathbb{A}^m$ as the variety of $r \times m$ -matrices over k , and we define

$\varphi(G, x) := (G, Gx)$ for $G \in \mathbb{A}^m$, $x \in V$.

Let $(G, b) \in \mathbb{A}^m \times \mathbb{A}^r$. Its fibre $\varphi^{-1}(G, b)$ corresponds to the intersection of V with r affine hyperplanes of $\mathbb{A}^n$ described by (G, b) .

Next we note that φ is dominating. By Noether's Normalization Lemma (Mumford), Chapter I, § 1, (Shafarevich), Chapter I, § 5, Theorem 9, there exists a linear map $\mathbb{A}^n \longrightarrow \mathbb{A}^r$ described by a $r \times n$ -matrix G such that the induced map $\mathbb{A}^n \longrightarrow V$ is finite. Fixing any point $b \in \mathbb{A}^r$, this means that there exist r affine hyperplanes of $\mathbb{A}^n$ described by (G, b) intersecting V in a nonempty finite set.

Hence $\varphi^{-1}(G, b)$ is nonempty and finite, whence, by the theorem of fibres of a morphism (Mumford), Chapter I, § 8, Theorem 2, (Shafarevich 1972), Chapter I, § 6, Theorem 7, $\dim \mathbb{A}^m \times V - \dim \overline{\varphi(\mathbb{A}^m \times V)} = 0$. Finally we conclude that $\overline{\varphi(\mathbb{A}^m \times V)} = \mathbb{A}^m \times \mathbb{A}^r$, whence φ is dominating.

So φ induces a field extension $k(\mathbb{A}^m \times \mathbb{A}^r) \subset k(\mathbb{A}^m \times V)$. Since $\dim \mathbb{A}^m \times \mathbb{A}^r = \dim \mathbb{A}^m \times V$ this field extension is finite.

The functions defined on an affine variety which are restrictions of the projections of the ambient space of the variety are usually called the coordinate functions of the variety.

Let $i=1, \dots, r$ and $j=1, \dots, m$.

We arrange the coordinate functions of $\mathbb{A}^m$ in a $r \times m$ -matrix $\Pi = (\pi_{ij})$.

Let $\theta = (\theta_1, \dots, \theta_n)$ be the n -tuple of the coordinate functions of V , and

let $\zeta = (\zeta_1, \dots, \zeta_r) := \Pi \theta$. φ maps the r last coordinate functions of $\mathbb{A}^m \times \mathbb{A}^r$ on $\zeta_1, \dots, \zeta_r$, therefore we identify $k(\mathbb{A}^m \times \mathbb{A}^r)$ with $k(\mathbb{A}^m)(\zeta)$.

With these notations we have the following

Lemma 1:

- (i) The field extension $k(A^m \times A^r) \subset k(A^m \times V)$ is separable algebraic.
- (ii) There is an open affine subvariety O of A^m such that the restriction of φ on $O \times V$ is a finite morphism $O \times V \rightarrow O \times A^r$.
- (iii) There are polynomials $F_1(Z_1, \dots, Z_r, T_1), \dots, F_n(Z_1, \dots, Z_r, T_n)$ in the indeterminates $Z_1, \dots, Z_r, T_1, \dots, T_n$ over $k(A^m)$ with $\deg_{T_j} F_j = \deg F_j > 0$ such that $F_j(\zeta, \theta_j) = 0$.

Proof: (i) By the proof of (Shafarevich 1972), Chapter I, § 3, Theorem 6, or by the proof of (Lang 1972), Chapter III, § 1, Theorem 1.1, we may assume without loss of generality that $\theta_1, \dots, \theta_n$ are separable algebraic over $k(\theta_1, \dots, \theta_r)$.

Hence there exist polynomials $P_{r+1}(T_1, \dots, T_r, T_{r+1}), \dots, P_n(T_1, \dots, T_r, T_n)$ in the indeterminates $T_1, \dots, T_n$ over k with $\frac{\partial P_{r+1}}{\partial T_{r+1}}(\theta_1, \dots, \theta_r, \theta_{r+1}) \neq 0, \dots, \frac{\partial P_n}{\partial T_n}(\theta_1, \dots, \theta_r, \theta_n) \neq 0$ such that $P_{r+1}(\theta_1, \dots, \theta_r, \theta_{r+1}) = 0, \dots, P_n(\theta_1, \dots, \theta_r, \theta_n) = 0$.

Expressing $\theta_1, \dots, \theta_r$ by $\zeta_1, \dots, \zeta_r$ and $\theta_{r+1}, \dots, \theta_n$ we obtain from

$P_{r+1}, \dots, P_n$ polynomials $Q_{r+1}(Z_1, \dots, Z_r, T_{r+1}, \dots, T_n), \dots, P_n(Z_1, \dots, Z_r, T_{r+1}, \dots, T_n)$ in the indeterminates $Z_1, \dots, Z_r, T_{r+1}, \dots, T_n$ over $k(A^m)$ such that

$$\det \begin{pmatrix} \frac{\partial Q_{r+1}}{\partial T_{r+1}}(\zeta, \theta_{r+1}, \dots, \theta_n) & \dots & \frac{\partial Q_{r+1}}{\partial T_n}(\zeta, \theta_{r+1}, \dots, \theta_n) \\ \vdots & & \vdots \\ \frac{\partial Q_n}{\partial T_{r+1}}(\zeta, \theta_{r+1}, \dots, \theta_n) & \dots & \frac{\partial Q_n}{\partial T_n}(\zeta, \theta_{r+1}, \dots, \theta_n) \end{pmatrix} \neq 0$$

and $Q_{r+1}(\zeta, \theta_{r+1}, \dots, \theta_n) = 0, \dots, Q_n(\zeta, \theta_{r+1}, \dots, \theta_n) = 0$, whence by (Lang 1969), Chapter X, § 7, Proposition 8, first $\theta_{r+1}, \dots, \theta_n$ and then $\theta_1, \dots, \theta_r$ are separable algebraic over $k(A^m)(\zeta)$. Since we identify $k(A^m)(\zeta)$ with $k(A^m \times A^r)$ we finally conclude that $k(A^m \times V) = k(A^m)(\theta)$ is separable algebraic over $k(A^m \times A^r)$.

(iii) implies (ii), therefore we show (iii). Since φ is dominating $\zeta_1, \dots, \zeta_r$ form a transcendence basis of $k(A^m \times V)$ over $k(A^m)$. Hence there exist nonzero polynomials $G_1(Z_1, \dots, Z_r, T_1), \dots, G_n(Z_1, \dots, Z_r, T_n)$ in the indeterminates $Z_1, \dots, Z_r, T_1, \dots, T_n$ over $k(A^m)$ such that $G_j(\zeta, \theta_j) = 0$ for $j=1, \dots, n$.

For the moment, fix j . Choose $c \in k$ such that

$$\deg_{T_j} G_j(Z_1 + cT_j, \dots, Z_r + cT_j, T_j) = \deg G_j.$$

Let G_j^* be the image of G_j under the automorphism of $k(\mathbb{A}^{rn})[Z_1, \dots, Z_r, T_j]$ which maps $\pi_{1j}, \dots, \pi_{rj}$ on $\pi_{1j} + c, \dots, \pi_{rj} + c$ and leaves the other coordinate functions of $\mathbb{A}^{rn}$ and $Z_1, \dots, Z_r, T_j$ fixed.

Similarly let $\zeta^* = (\zeta_1^*, \dots, \zeta_r^*)$ be the image of ζ under the automorphism of $k(\mathbb{A}^{rn} \times V)$ which maps $\pi_{1j}, \dots, \pi_{rj}$ on $\pi_{1j} + c, \dots, \pi_{rj} + c$ and leaves the other coordinate functions of $\mathbb{A}^{rn} \times V$ fixed. Applying this isomorphism on the expression $G_j(\zeta, \theta_j) = 0$, we conclude $G_j^*(\zeta^*, \theta_j) = 0$.

Finally put $F_j(Z_1, \dots, Z_r, T_j) := G_j^*(Z_1 + cT_j, \dots, Z_r + cT_j, T_j)$. Then we have

$$\deg_{T_j} F_j = \deg F_j > 0 \quad \text{and}$$

$$F_j(\zeta, \theta_j) = G_j^*(\zeta^*, \theta_j) = 0$$

as we wanted.

Remark 1: Lemma 1(i) is a well known theorem from algebraic geometry (compare (Samuel 1967), Chapter I, § 8.3.), whereas (ii) is some version of the Noether Normalization Theorem (compare (Lang 1972), Chapter II, § 1, Theorem 1').

As we have shown, $\varphi: \mathbb{A}^{rn} \times V \longrightarrow \mathbb{A}^{rn} \times \mathbb{A}^r$ is a dominating morphism of a $(rn+r)$ -dimensional affine variety in the $(rn+r)$ -dimensional affine space. Furthermore, by Lemma 1 (i), the field extension $k(\mathbb{A}^{rn} \times \mathbb{A}^r) \subset k(\mathbb{A}^{rn} \times V)$ induced by φ is separable.

So we can apply Proposition 1 to φ . This leads us to the following

Definition 1: Let V be a closed subvariety of $\mathbb{A}^n$ with $\dim V = r$. Then we write

$$\begin{aligned} \deg_{\mathbb{A}^n} V &:= [k(\mathbb{A}^{rn} \times V) : k(\mathbb{A}^{rn} \times \mathbb{A}^r)] = \\ &= \sup \{ \# H_1 \cap \dots \cap H_r \cap V; H_1, \dots, H_r \text{ affine hyperplanes} \\ &\quad \text{of } \mathbb{A}^n \text{ such that } H_1 \cap \dots \cap H_r \cap V \text{ is finite} \} \\ &= \sup \{ \# E \cap V; E \text{ (n-r)-dimensional affine subspace} \\ &\quad \text{of } \mathbb{A}^n \text{ such that } E \cap V \text{ is finite} \}. \end{aligned}$$

We call $\deg_{\mathbb{A}^n} V$ the degree of V .

Remark 2: 1. Proposition 1 (ii) suggests to extend the notion of degree to open subsets of closed subvarieties of $\mathbb{A}^n$. For almost all $(n-r)$ -dimensional affine subspaces of $\mathbb{A}^n$ (described as elements of a nonempty open subset of $\mathbb{A}^m \times \mathbb{A}^r$) intersect a given open subset of V in $\deg_{\mathbb{A}^n} V$ many points. Nevertheless, for our purposes it is convenient to extend the notion of degree on arbitrary constructible (i.e. Boolean combination of closed) subsets of $\mathbb{A}^n$:

Let $X \subset \mathbb{A}^n$ be constructible and C be the set of the components of $\bar{X}$. We define

$$\deg_{\mathbb{A}^n} X := \sum_{C \in C} \deg_{\mathbb{A}^n} C.$$

2. Let $X \subset \mathbb{A}^n$ be constructible and E an affine subspace of $\mathbb{A}^n$. Then

$$\deg_{\mathbb{A}^n} X \cap E \leq \deg_{\mathbb{A}^n} X.$$

Proof: Since E is an intersection of $\text{codim}_{\mathbb{A}^n} E := n - \dim E$ many hyperplanes, we may assume without loss of generality $\text{codim}_{\mathbb{A}^n} E = 1$, i.e. E an affine hyperplane. Furthermore, we may assume without loss of generality that X is an irreducible closed subset of $\mathbb{A}^n$. We only have to consider the case where E intersects X properly, i.e. $X \not\subset E$. Let $X \cap E = \bigcup_{1 \leq i \leq s} C_i$ be an irredundant decomposition of $X \cap E$ in irreducible components.

For $i=1, \dots, s$ put $X_i = C_i - \bigcup_{1 \leq j < i} C_j$. The X_i are nonempty, locally closed (and hence constructible) subvarieties of $\mathbb{A}^n$ with $\dim X_i = \dim C_i = \dim X - 1$ and $\deg_{\mathbb{A}^n} X_i = \deg_{\mathbb{A}^n} C_i$. The X_i form a partition of $X \cap E$.

By 1. of this remark, we can choose an affine subspace of $\mathbb{A}^n$, say F , with $\dim F = n - \dim X + 1$ such that $\#X_i \cap F = \deg_{\mathbb{A}^n} X_i = \deg_{\mathbb{A}^n} C_i$, $i=1, \dots, s$.

Then $\deg_{\mathbb{A}^n} X \cap E = \sum_{1 \leq i \leq s} \deg_{\mathbb{A}^n} C_i = \sum_{1 \leq i \leq s} \#X_i \cap F = \#X \cap E \cap F \leq \deg_{\mathbb{A}^n} X$ by Proposition 1 (i).

3. It can easily be verified that $\deg_{\mathbb{A}^n} \mathbb{A}^n = 1$, and that the degree of any hypersurface of $\mathbb{A}^n$ equals the degree of its defining polynomial. Degree is never zero.

In general, it is clear from the context in which affine space the constructible set X is thought to be embedded. In these cases we don't mention the ambient space $\mathbb{A}^n$, and we simply write $\deg X$ for the degree of X in $\mathbb{A}^n$. The notion of degree for constructible sets is invariant under affine linear isomorphisms of the ambient spaces, although it is not under isomorphisms in general.

The following lemma says how degree behaves under affine linear maps.

Lemma 2: Let $\varphi: \mathbb{A}^n \rightarrow \mathbb{A}^m$ be affine linear, $X \subset \mathbb{A}^n$ constructible. Then $\deg \varphi(X) \leq \deg X$.

Proof: Without loss of generality, we may assume that X is an irreducible closed subset of $\mathbb{A}^n$. By (Mumford), Chapter I, § 8, Theorem 3(i), and Remark 2.1 we can choose a $\overline{\varphi(X)}$ -dimensional affine subspace F of $\mathbb{A}^n$ such that $\# \varphi(X) \cap F = \deg \varphi(X)$. Since φ is affine linear $E := \varphi^{-1}(F)$ is an affine subspace of $\mathbb{A}^n$. Then we have by Remark 2.2

$$\deg \varphi(X) = \# \varphi(X) \cap F \leq \# \text{components of } X \cap E \leq \deg X \cap E \leq \deg X.$$

Next we want to give a Bezout-like estimate for the degree of the intersection of constructible subsets of affine spaces. For this purpose we show

Proposition 2: Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be constructible. Then $\deg X \times Y = \deg X \cdot \deg Y$.

Proof: Let $\bar{X} = \cup V_i$ and $\bar{Y} = \cup W_j$ be the decompositions of $\bar{X}$ and $\bar{Y}$ into their irreducible components V_i and W_j .

We have $\overline{X \times Y} = \bar{X} \times \bar{Y}$, and so the $V_i \times W_j$ are the components of $\overline{X \times Y}$.

Hence $\deg X \times Y = \sum_{i,j} \deg V_i \times W_j$, and Proposition 2 follows if we can show $\deg V_i \times W_j = \deg V_i \cdot \deg W_j$.

So we may assume without loss of generality that X and Y are irreducible closed subsets of $\mathbb{A}^m$ and $\mathbb{A}^n$ respectively with $\dim X = r$ and $\dim Y = s$.

We embed $\mathbb{A}^{rm+sn}$ into $\mathbb{A}^{(r+s)(m+n)}$, reading $\mathbb{A}^{rm+sn}$ as the variety of $(r+s) \times (m+n)$ -matrices with zeroes in the left bottom and the right top corner $s \times m$ - and $r \times n$ -rectangles.

Let $\mathbb{A}^{rm+sn} \times X \times Y \rightarrow \mathbb{A}^{(r+s)(m+n)} \times X \times Y$ be the product of this morphism with the identity map on $X \times Y$. Similarly let

$$\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s} \rightarrow \mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s} \quad \text{be the product of the embedding}$$

$$\mathbb{A}^{rm+sn} \rightarrow \mathbb{A}^{(r+s)(m+n)} \quad \text{with the identity on } \mathbb{A}^{r+s}.$$

The elements of $\mathbb{A}^{(r+s)(m+n)}$ (which we read as $(r+s) \times (m+n)$ -matrices) operate on $X \times Y$ mapping $X \times Y$ into $\mathbb{A}^{r+s}$.

To $G \in \mathbb{A}^{(r+s)(m+n)}$, $x \in X, y \in Y$ we assign $(G, G(x, y))$ defining thus a morphism $\mathbb{A}^{(r+s)(m+n)} \times X \times Y \longrightarrow \mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}$.

This morphism is dominating.

Let the morphisms $\mathbb{A}^{rm} \times X \longrightarrow \mathbb{A}^{rm} \times \mathbb{A}^r$ and $\mathbb{A}^{sn} \times Y \longrightarrow \mathbb{A}^{sn} \times \mathbb{A}^s$ (considering the elements of $\mathbb{A}^{rm}$ and $\mathbb{A}^{sn}$ as $r \times m$ - and $s \times n$ -matrices operating on X and Y respectively) be analogously defined.

Finally, let $\mathbb{A}^{rm+sn} \times X \times Y \longrightarrow \mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s}$ be the morphism obtained from the product of $\mathbb{A}^{rm} \times X \longrightarrow \mathbb{A}^{rm} \times \mathbb{A}^r$ and $\mathbb{A}^{sn} \times Y \longrightarrow \mathbb{A}^{sn} \times \mathbb{A}^s$ after suitable reordering of the factors.

This morphism is dominating too, since $\mathbb{A}^{rm} \times X \longrightarrow \mathbb{A}^{rm} \times \mathbb{A}^r$ and $\mathbb{A}^{sn} \times Y \longrightarrow \mathbb{A}^{sn} \times \mathbb{A}^s$ are dominating.

The field extension $k(\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s}) \subset k(\mathbb{A}^{rm+sn} \times X \times Y)$ is separable algebraic since by Lemma 1(i) $k(\mathbb{A}^{rm} \times \mathbb{A}^r) \subset k(\mathbb{A}^{rm} \times X)$ and $k(\mathbb{A}^{sn} \times \mathbb{A}^s) \subset k(\mathbb{A}^{sn} \times Y)$ are separable algebraic.

Furthermore we have $[k(\mathbb{A}^{rm+sn} \times X \times Y) : k(\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s})] = \deg X \cdot \deg Y$.

So we obtain a commutative diagram

$$\begin{array}{ccc} \mathbb{A}^{(r+s)(m+n)} \times X \times Y & \longrightarrow & \mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s} \\ \uparrow & & \uparrow \\ \mathbb{A}^{rm+sn} \times X \times Y & \longrightarrow & \mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s} \end{array}$$

Let q be the ideal of elements of $k[\mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}]$ vanishing on $\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s}$. q generates in $k[\mathbb{A}^{(r+s)(m+n)} \times X \times Y]$ the ideal of functions vanishing on $\mathbb{A}^{rm+sn} \times X \times Y$.

Let $P := k[\mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}] - q$ and $R := P^{-1} k[\mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}]$, $S := P^{-1} k[\mathbb{A}^{(r+s)(m+n)} \times X \times Y]$

R is a normal and local ring with maximal ideal, say m , and residue class field $k(\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s})$.

Assume $R \subset S$ integral (we will show this later). Then S is local too with maximal ideal Sm and residue class field $k(\mathbb{A}^{(r+s)(m+n)} \times X \times Y)$.

The canonical morphism $R/m \longrightarrow R/m \otimes_R S$ is the embedding of $k(\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s})$ into $k(\mathbb{A}^{(r+s)(m+n)} \times X \times Y)$ induced by the bottom morphism of the diagram. So, $R/m \longrightarrow R/m \otimes_R S$ is a separable algebraic field extension of degree $\deg X \cdot \deg Y$.

Take $s \in S$ such that $1 \otimes s$ is a primitive element generating $R/m \otimes_R S$ over R/m . Since R is normal, $R[s]$ is a free R -module. We show $R[s] = S$.

Tensoring the exact sequence

$$R[s] \longrightarrow S \longrightarrow \text{Coker} \longrightarrow 0$$

with R/m , we obtain $R/m \otimes_R \text{Coker} = 0$, hence $\text{Coker} = 0$ by Nakayama's Lemma ((Atiyah-Macdonald 1969), p. 21, prop. 2.6). So $R[s] \longrightarrow S$ is surjective, in other words $R[s] = S$. Now S is a free R -module, and we have

$$\begin{aligned} \deg X \times Y &= [k(\mathbb{A}^{(r+s)(m+n)} \times X \times Y) : k(\mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s})] = \\ &= \text{rank}_R S = [R/m \otimes_R S : R/m] = \deg X \cdot \deg Y. \end{aligned}$$

Now we are going to show $R \subset S$ integral.

For the rest of the proof let $i=1, \dots, r+s$, $j=1, \dots, m+n$ and $k=r+1, \dots, m, m+s+1, \dots, m+n$. We write $\Pi = (\pi_{ij})$ for the $(r+s) \times (m+n)$ -matrix of coordinate functions of $\mathbb{A}^{(r+s)(m+n)}$, $\theta = (\theta_1, \dots, \theta_{m+n})$ for the $m+n$ -tuple of coordinate functions of $X \times Y$, where $\theta_1, \dots, \theta_m$ correspond to X , and $\theta_{m+1}, \dots, \theta_{m+n}$ to Y . Let $\zeta = (\zeta_1, \dots, \zeta_{r+s})$ with $\zeta_i = \sum_{1 \leq j \leq m+n} \pi_{ij} \theta_j$. The π_{ij} and the ζ_i are contained in R . Let I be the subring of R obtained by localizing the ring $k[\mathbb{A}^{(r+s)(m+n)}]$, generated by the π_{ij} over k , at its intersection with m . I is local with maximal ideal, say n , and residue class field $\bar{I} := k(\mathbb{A}^{rm+sn})$.

Furthermore $k(\mathbb{A}^{rm})$ and $k(\mathbb{A}^{sn})$, the fields generated over k by the elements of $\bar{I}$ in the left top and the right bottom $r \times m$ - and $s \times n$ -rectangles, i.e. by the π_{ij} with $i \leq r$, $j \leq m$ and the π_{ij} with $r < i$, $m < j$, are contained in I .

Since $I[\zeta] \subset R$ and $S = R[\theta]$ it suffices to show that $\theta_1, \dots, \theta_{m+n}$ are integral over $I[\zeta]$.

In the sequel we shall consider polynomials over I . For such a polynomial, say F , we denote by $\bar{F}$ its residue class in the polynomial ring in the same indeterminates as F over $\bar{I}$.

For $i = 1, \dots, r$ let $\zeta_i^X := \sum_{1 \leq j \leq m} \pi_{ij} \theta_j$ and for $i = r+1, \dots, r+s$ let $\zeta_i^Y := \sum_{m \leq j \leq m+n} \pi_{ij} \theta_j$. From Lemma 1 (iii) we see that there exist polynomials $F_k^X(Z_1^X, \dots, Z_r^X, T_k)$, $k = r+1, \dots, m$, in the indeterminates $Z_1^X, \dots, Z_r^X, T_k$ over $k(A^m)$, and polynomials $F_k^Y(Z_{r+1}^Y, \dots, Z_{r+s}^Y, T_k)$, $k = m+s+1, \dots, m+n$, in the indeterminates $Z_{r+1}^Y, \dots, Z_{r+s}^Y, T_k$ over $k(A^{sn})$, such that $\deg_{T_k} F_k^X = \deg F_k^X > 0$, $F_k^X(\zeta_1^X, \dots, \zeta_r^X, \theta_k) = 0$ and $\deg_{T_k} F_k^Y = \deg F_k^Y > 0$, $F_k^Y(\zeta_{r+1}^Y, \dots, \zeta_{r+s}^Y, \theta_k) = 0$ respectively.

We express each ζ_i^X, ζ_i^Y as linear combination of $\zeta_1, \dots, \zeta_{r+s}$ and $\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}$ over I such that the coefficients of $\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}$ are in n . Introducing for $\zeta_1, \dots, \zeta_{r+s}$ new indeterminates $Z_1, \dots, Z_{r+s}$, we substitute in the F_k^X, F_k^Y for the ζ_i^X, ζ_i^Y the corresponding linear combinations of $Z_1, \dots, Z_{r+s}$ and $T_{r+1}, \dots, T_m, T_{m+s+1}, \dots, T_{m+n}$. Thus we obtain new polynomials, say $F_{r+1}, \dots, F_m, F_{m+s+1}, \dots, F_{m+n}$ in the indeterminates $Z_1, \dots, Z_{r+s}, T_{r+1}, \dots, T_m, T_{m+s+1}, \dots, T_{m+n}$ over I with $F_k(\zeta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}) = 0$. By construction, note that $\bar{F}_k$ contains no other indeterminates than $Z_1, \dots, Z_{r+s}, T_k$ and that $\deg_{T_k} \bar{F}_k = \deg F_k > 0$.

Let ℓ range over $r+1, \dots, m, m+s+1, \dots, m+n$ and write $\ell^* := \ell - 1$ for $\ell \neq m+s+1$ and $\ell^* = m$ for $\ell = m+s+1$. Define polynomials $F_{r+1}^\ell, \dots, F_k^\ell, \dots, F_\ell^\ell$ in the indeterminates $Z_1, \dots, Z_{r+1}, T_{r+1}, \dots, T_\ell$ over I recursively as follows:

$$F_{r+1}^{m+n} := F_{r+1}, \dots, F_k^{m+n} := F_k, \dots, F_{m+n}^{m+n} := F_{m+n}.$$

Considering the F_k^ℓ as polynomials in T_ℓ over $I[Z_1, \dots, Z_{r+s}, T_{r+1}, \dots, T_{\ell^*}]$ of formal degree $\deg F_k^\ell$, let for $k \leq \ell^*$ $F_k^{\ell^*}$ be the resultant of F_k^ℓ, F_ℓ^ℓ .

Note that the degrees of the elements of Sylvester's matrix corresponding to $F_{\ell}^{\ell}, F_k^{\ell}$ are bounded by the "weight" of their respective position in the matrix. So it is easy to verify - compare (van der Waerden 1971), p. 108 § 35, ex. 1 - that $\deg F_k^{\ell*} \leq \deg F_{\ell}^{\ell} \cdot \deg F_k^{\ell}$ holds.

By means of this inequality and using the fact that $\bar{F}_k^{\ell}$ contains no other indeterminates than $Z_1, \dots, Z_{r+s}, T_k$, we see by recursion on ℓ that $\deg_{T_k} \bar{F}_k^{\ell} = \deg F_k^{\ell} > 0$. Also by recursion on ℓ we see $F_k^{\ell}(\zeta, \theta_{r+1}, \dots, \theta_{\ell}) = 0$.

Now consider $F_{r+1}^{r+1}, \dots, F_m^m, F_{m+s+1}^{m+s+1}, \dots, F_{m+n}^{m+n}$.

Since $F_{\ell}^{\ell}(\zeta, \theta_{r+1}, \dots, \theta_{\ell}) = 0$ and $\deg_{T_{\ell}} F_{\ell}^{\ell} = \deg F_{\ell}^{\ell} > 0$, we conclude that θ_{ℓ} is integral over $I[\zeta, \theta_{r+1}, \dots, \theta_{\ell*}]$.

Consequently, $\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}$ are integral over $I[\zeta]$.

The remaining $\theta_1, \dots, \theta_r, \theta_{m+1}, \dots, \theta_{m+s}$ can be expressed as linear combinations of the $\zeta_1, \dots, \zeta_{r+s}$ and the $\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}$ over I . So all the $\theta_1, \dots, \theta_{m+n}$ are integral over $I[\zeta]$, whence $R \subset S$ is integral.

Using some valuation theory (compare (Atiyah-Macdonald 1969), Chapter 5, and (Lang 1969), Chapter XII, §§ 4, 5, 6) the last part of this proof can be simplified as follows:

Let v be any (multiplicatively written) valuation of $k(A^{(r+s)(m+n)} \times X \times Y)$ lying above R (i.e. with $m = \{x \in R; v(x) < 1\}$). Let $o \subset k(A^{(r+s)(m+n)} \times X \times Y)$ be the valuation ring of v . We choose θ_{ℓ} from $\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n}$ such that $v(\theta_{\ell}) \geq v(\theta_k)$ for each $k = r+1, \dots, m, m+s+1, \dots, m+n$.

Without loss of generality we may assume $\theta_{\ell} \neq 0$. So, each $\frac{\theta_k}{\theta_{\ell}}$ is in the valuation ring of v .

We consider $F_{\ell}(\zeta, T_{r+1}, \dots, T_m, T_{m+s+1}, \dots, T_{m+n})$ as a polynomial

$G \in R[\frac{T_{r+1}}{T_{\ell}}, \dots, \frac{T_m}{T_{\ell}}, \frac{T_{m+s+1}}{T_{\ell}}, \dots, \frac{T_{m+n}}{T_{\ell}}, T_{\ell}]$. From the fact that $\bar{F}_{\ell}$ depends only on $Z_1, \dots, Z_{r+s}$ and T_{ℓ} we conclude that the leading coefficient of $G(\frac{\theta_{r+1}}{\theta_{\ell}}, \dots, \frac{\theta_m}{\theta_{\ell}}, \frac{\theta_{m+s+1}}{\theta_{\ell}}, \dots, \frac{\theta_{m+n}}{\theta_{\ell}}, T_{\ell}) \in o[T_{\ell}]$ is a unit of o .

So, since $G(\frac{\theta_{r+1}}{\theta_{\ell}}, \dots, \frac{\theta_m}{\theta_{\ell}}, \frac{\theta_{m+s+1}}{\theta_{\ell}}, \dots, \frac{\theta_{m+n}}{\theta_{\ell}}, \theta_{\ell}) = 0$, we see that θ_{ℓ} is integral over o . Hence $\theta_{\ell} \in o$, and, by the choice of θ_{ℓ} ,

$\theta_{r+1}, \dots, \theta_m, \theta_{m+s+1}, \dots, \theta_{m+n} \in o$. Finally we have $\theta_1, \dots, \theta_{m+n} \in o$.

So we have seen that the valuation ring of any valuation v of $k(\mathbb{A}^{(r+s)(m+n)} \times X \times Y)$ lying above R contains $\theta_1, \dots, \theta_{m+n}$. From this we conclude by (Atiyah-Macdonald 1969), Chapter 5, Corollary 5.22, or (Lang 1969), Chapter XII, § 4, Proposition 15, that $\theta_1, \dots, \theta_{m+n}$ are integral over R .

The geometrical idea of the proof of Proposition 2 is roughly the following:

We consider the fibres of the morphism

$\mathbb{A}^{(r+s)(m+n)} \times X \times Y \longrightarrow \mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}$. We construct an open set $U \subset \mathbb{A}^{(r+s)(m+n)} \times \mathbb{A}^{r+s}$ with $U \cap \mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s} \neq \emptyset$ such that the fibres of the points of U are finite, unramified, and have no "component at infinity". Then the cardinality of each such fibre is $\deg X \times Y$. But since U intersects $\mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s}$ there is also a point of $U \cap \mathbb{A}^{rm+sn} \times \mathbb{A}^{r+s}$ with fibre of cardinality $\deg X \cdot \deg Y$, whence $\deg X \times Y = \deg X \cdot \deg Y$.

We conclude this purely algebraic geometrical part of our paper by

Theorem 1: Let $X, Y \subset \mathbb{A}^n$ be constructible.

Then $\deg X \cap Y \leq \deg X \cdot \deg Y$ ("Bezout - Inequality").

Proof: As in the proof of Proposition 2, without loss of generality, we may assume that X and Y are closed subvarieties of $\mathbb{A}^n$. The diagonal Δ of $\mathbb{A}^n \times \mathbb{A}^n$ is a linear subspace of $\mathbb{A}^n \times \mathbb{A}^n$. Choose any projection $\pi: \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{A}^n$. π maps $(X \times Y) \cap \Delta$ on $X \cap Y$, whence, by Proposition 2, Remark 2, and Lemma 2, the theorem follows.

II. Definability

We are going to give estimates for the number of sets definable by first order formulas in a fixed set of variables, starting from a finite set x of constructible subsets of $\mathbb{A}^n$, which we consider as the interpretations of the atomic formulas of our language. At the same time we are going to estimate the number of points of any such definable set in case that it is finite. We begin with some terminology including our final version of the notion of degree.

Let X be a finite set of constructible subsets of $\mathbb{A}^n$. We denote by $D(X)$ the boolean algebra of subsets of $\mathbb{A}^n$ generated by X , and we call a subset of $\mathbb{A}^n$ X -definable if it is in $D(X)$.

We write

$$Z(X) := \{Z \in D(X); \exists M \subset X \ Z = \bigcap_{X \in M} X \cap \bigcap_{X' \in X-M} (\mathbb{A}^n - X') \neq \emptyset\}.$$

The elements of $Z(X)$ are the atoms of $D(X)$. $Z(X)$ is a finite partition of $\mathbb{A}^n$. We call $Z(X)$ the cell division of $\mathbb{A}^n$ by X , and we call its elements X -cells. A subset of $\mathbb{A}^n$ is X -definable iff it is the union of X -cells.

We write

$$C(X) := \{C; C \text{ component of some } \bar{X} \text{ with } X \in X\}$$

and

$$\deg X := \sum_{C \in C(X)} \deg C.$$

We call $\deg X$ the degree of X .

Note $\#C(X) \leq \deg X$ and $\deg D(X) = \deg Z(X)$.

We have $\deg X \leq \sum_{X \in X} \deg X$ but not necessarily equality.

Finally, we write

$$\text{grd } X := \min \{ \deg V; V \text{ a finite set of irreducible closed subsets of } \mathbb{A}^n \text{ with } X \subset D(V) \}.$$

We call $\text{grd } X$ the grade (Erzeugungsgrad) of X .

Note $\text{grd } X = \text{grd } Z(X) = \text{grd } D(X)$. $\text{grd } X$ is never zero except for $X \subset \{\emptyset, \mathbb{A}^n\}$.

If X consists of closed subsets of $\mathbb{A}^n$, then its elements are definable by $C(X)$. Hence $\text{grd } X \leq \deg X$ in this case. Equality holds for example if X consists of irreducible hypersurfaces of $\mathbb{A}^n$. (To prove this, we choose a finite set V of irreducible closed subsets of $\mathbb{A}^n$ with $\deg V = \text{grd } X$, such that each element of X is V -definable. We will show $X \subset V$.

Then, by $\deg X \leq \deg V = \text{grd } X$ we have $\text{grd } X = \deg X$.

Let X be any element of $\mathcal{X}$. X is a union of V -cells, say $X = Z_1 \cup \dots \cup Z_s$ with $Z_k \in \mathcal{Z}(V)$, $k=1, \dots, s$. Since X is closed and irreducible, we may assume

$$X = \bar{Z}_1 = \overline{\bigcap_{V \in M} V \cap \bigcap_{V' \in V \setminus M} (A^n - V')} = \bigcap_{V \in M} V \quad \text{for some } M \subset V. \quad \text{Since } X \text{ is a hyper-}$$

surface, this is only possible in case $M = \{X\}$. So we have $X \in V$.)

The following example illustrates that $\text{grd } X$ can be very small compared with $\deg X$.

Let V and W be irreducible closed subsets of A^n and $X = \{V \times W\}$, a singleton consisting of the irreducible closed subset $V \times W$ of $A^n \times A^n$. Then, by Proposition 2 we have $\deg X = \deg V \times W = \deg V \cdot \deg W$. On the other side we have $\text{grd } X \leq \deg V + \deg W$. So, if V and W have high degrees, $\text{grd } X$ is essentially smaller than $\deg X$.

With these notations we have

Theorem 2: Let X be a finite constructible subset of A^n . Then

- (i) $\deg D(X) \leq (1 + \text{grd } X)^n$
- (ii) $\# \mathcal{Z}(X) \leq (1 + \text{grd } X)^n$
- (iii) any X -definable finite subset of A^n contains at most $(1 + \text{grd } X)^n$ points
- (iv) $\# D(X) \leq 2^{(1 + \text{grd } X)^n}$.

Proof: First we show (i) $\Rightarrow$ (iii) and (ii) $\Rightarrow$ (iv).

Any finite subset of A^n is Zariski closed, and its points are its components.

Hence the points of a X -definable finite subset of A^n are in $C(D(X))$.

By $\# C(D(X)) \leq \deg D(X)$ (iii) follows from (i).

(ii) $\Rightarrow$ (iv) is obvious since each element of $D(X)$ is a finite union of X -cells.

To show (i) and (ii) we choose a finite set V of irreducible closed subsets of A^n with $\deg V = \text{grd } X$, such that every $X \in \mathcal{X}$ is V -definable.

Since the cell division $\mathcal{Z}(V)$ is a refinement of the cell division $\mathcal{Z}(X)$ of A^n , we have

$$C(D(X)) \subset C(\mathcal{Z}(V))$$

and hence

$$(1) \quad \deg D(X) \leq \deg \mathcal{Z}(V).$$

Furthermore, we have by the same argument

$$(2) \quad \# Z(X) \leq \# Z(V) .$$

To prove (i) it suffices to show

$$(3) \quad \deg Z(V) \leq (1 + \deg V)^n ,$$

for then, by (1) and $\deg V = \text{grd } X$, we have

$$\deg D(X) \leq \deg Z(V) \leq (1 + \deg V)^n = (1 + \text{grd } X)^n .$$

Finally, to prove (ii) it suffices to show

$$(4) \quad \# Z(V) \leq \# C(Z(V))$$

for then, by (2) and (3), we have

$$\# Z(X) \leq \# Z(V) \leq \# C(Z(V)) \leq \deg Z(V) \leq (1 + \deg V)^n = (1 + \text{grd } X)^n .$$

We are going to show (3).

First note

$$(5) \quad C(Z(V)) = \{C; \exists M \subset V \text{ such that } C \text{ is a component of } \bigcap_{V \in M} V\} .$$

(The inclusion $\subset$ in (5) is obvious. To show $\supset$ let for some $M \subset V$ C be a component of $\bigcap_{V \in M} V$. Then C is also a component of

$$\bigcap_{V \in M_0} V = \frac{\bigcap_{V \in M_0} V \cap \bigcap_{V \in V-M_0} (A^n - V)}{(A^n - V)} , \text{ where } M_0 = \{V \in V; C \subset V\} .$$

So we have $C \in C(Z(V))$.)

Let $c_i := \{C \in C(Z(V)); \text{codim } C = i\}$, $i = 0, \dots, n$, and

$$d_i := \sum_{0 \leq k \leq i} \deg c_k = \deg \bigcup_{0 \leq k \leq i} c_k = \sum_{C \in \bigcup_{0 \leq k \leq i} c_k} \deg C .$$

We have $d_0 = 1$.

Let $i > 0$ and let $C \in c_i$. By (5) C is a component of $\bigcap_{V \in M} V$ for some $M \subset V$.

We choose M such that for some $V^* \in M$, C is not component of $\bigcap_{\substack{V \in M \\ V \neq V^*}} V$.

Then there exists a component C^* of $\bigcap_{\substack{V \in M \\ V \neq V^*}} V$ with $C \not\subset C^*$, such that C is a component of $C^* \cap V^*$.

By (5) we have $C^* \in C(Z(V))$ and by $C \not\subset C^*$ we have $\text{codim } C^* < \text{codim } C = i$,

hence $C^* \in \bigcup_{0 \leq k < i} c_k$.

From this we conclude for $i > 0$:

$$c_i \subset \{C; C \text{ component of } C^* \cap V^*, C^* \in \bigcup_{0 \leq k < i} c_k, V^* \in V\}$$

and by the Bezout Inequality (Theorem 1)

$$\begin{aligned}
 d_i &= \sum_{0 \leq k \leq i} \deg c_k = d_{i-1} + \deg c_i \leq d_{i-1} + \sum_{\substack{C^* \in \bigcup_{0 \leq k < i} C_k \\ V^* \in V}} \deg C^* \cap V^* \\
 &\leq d_{i-1} + \sum_{\substack{C^* \in \bigcup_{0 \leq k < i} C_k \\ V^* \in V}} \deg C^* \cdot \deg V^* = \\
 &= d_{i-1} + \sum_{C^* \in \bigcup_{0 \leq k < i} C_k} \deg C^* \cdot \sum_{V^* \in V} \deg V^* = \\
 &= d_{i-1} + d_{i-1} \cdot \deg V = d_{i-1} (1 + \deg V) .
 \end{aligned}$$

By induction on i we have then $d_i \leq (1 + \deg V)^i$ and finally

$$\deg Z(V) = \sum_{0 \leq i \leq n} \deg c_i = d_n \leq (1 + \deg V)^n .$$

This proves (3) and (i).

Now we are going to show (4).

To each $Z \in \mathcal{Z}(V)$ with $Z = \bigcap_{V \in M} V_M \cap (\mathbb{A}^n - V^*)$ for some $M \subset V$ we consider $c(\{Z\}) = \{C; C \text{ component of } \bigcap_{V \in M} V \text{ with } C \cap Z \neq \emptyset\}$.

For $Z, Z^* \in \mathcal{Z}(V)$ with $Z \neq Z^*$ we have $c(\{Z\}) \cap c(\{Z^*\}) = \emptyset$.

Otherwise there is some $C \in c(\{Z\}) \cap c(\{Z^*\})$. For this C we have $C \cap Z \neq \emptyset$ and $C \cap Z^* \neq \emptyset$. But $C \cap Z$ and $C \cap Z^*$ are open subsets of C , hence, by the irreducibility of C , $C \cap Z \cap Z^* \neq \emptyset$, a contradiction.

Finally we have

$$\#Z(V) \leq \sum_{Z \in \mathcal{Z}(V)} \#c(\{Z\}) = \# \bigcup_{Z \in \mathcal{Z}(V)} c(\{Z\}) \leq \#c(Z(V)) ,$$

whence (4) and (ii).

Let $F_1, \dots, F_s \in k[X_1, \dots, X_n]$ be polynomials in the indeterminates $X_1, \dots, X_n$ over k and let X consist of the hypersurfaces of $\mathbb{A}^n$ defined by the equations $F_k = 0$, $k = 1, \dots, s$.

We say $(F_1, \dots, F_s)$ -definable instead of X -definable and $(F_1, \dots, F_s)$ -cell instead of X -cell.

With these notations, the following corollary is a down-to-earth version of Theorem 2.

Corollary 1: The total number of components of $(F_1, \dots, F_s)$ -definable closed subsets of $\mathbb{A}^n$ and the number of $(F_1, \dots, F_s)$ -cells are bounded by $(1+d)^n$, where $d = \sum_{1 \leq k \leq s} \deg F_k$.

Consequently, a $(F_1, \dots, F_s)$ -definable finite subset of $\mathbb{A}^n$ contains at most $(1+d)^n$ points, and the number of $(F_1, \dots, F_s)$ -definable subsets of $\mathbb{A}^n$ does not exceed $2(1+d)^n$.

Proof: Obvious by Theorem 2.

Remark 3: 1. A simple minded counting would yield a bound of 2^s for the number of $(F_1, \dots, F_s)$ - cells and a simple minded application of the Bezout-Inequality would yield a similar bound of d^s for the cardinality of a $(F_1, \dots, F_s)$ - definable finite subset of $\mathbb{A}^n$.

Since in the typical applications s is large compared to n Corollary 1 gives a much better bound.

2. Furthermore, for n fixed, the bounds of Theorem 2 and Corollary 1 are asymptotically optimal. As an example consider

$$F_1 := X_1^d - 1, \dots, F_n := X_n^d - 1, \quad \text{char } k \nmid d.$$

Then $\#\{x \in \mathbb{A}^n; F_1(x) = 0, \dots, F_n(x) = 0\} = d^n$, whereas our bound is $(1+nd)^n$ in this case.

Next we are going to show that for the determination of $\text{grd } x$ we can restrict ourselves without too severe loss of precision to generating sets v consisting of hypersurfaces (Theorem 3).

We first show a lemma using the following

Fact: For given distinct elements $z_1, \dots, z_s \in \mathbb{A}^n$, there exists a nonempty open set $U \subset \mathbb{A}^n$ such that, with respect to the map $U \times \mathbb{A}^n \rightarrow \mathbb{A}^1$ defined by reading the elements of U as linear forms on $\mathbb{A}^n$, we have for each $g \in U$

$$g z_k \neq g z_\ell \quad \text{for } k \neq \ell.$$

Proof: Consider for each $k \neq \ell$ the nonempty, open set

$$U_{k\ell} := \{g \in \mathbb{A}^n; g z_k \neq g z_\ell\} \subset \mathbb{A}^n. \quad \text{Put } U := \bigcap_{1 \leq k \neq \ell \leq s} U_{k\ell}.$$

Lemma 3: Let V be a closed subvariety of $\mathbb{A}^n$ with $\dim V = r$ and let $x_1, \dots, x_s \in \mathbb{A}^n - V$. Then there exists a linear map $\varphi: \mathbb{A}^n \rightarrow \mathbb{A}^{r+1}$ with $\varphi(x_1), \dots, \varphi(x_s) \notin \overline{\varphi(V)}$ and $\dim \overline{\varphi(V)} = r$.

Proof: By Lemma 1 (ii) choose a linear map $\varphi_0: \mathbb{A}^n \rightarrow \mathbb{A}^r$ inducing a finite and surjective morphism $V \rightarrow \mathbb{A}^r$. Then, for $y_1 := \varphi_0(x_1), \dots, y_s := \varphi_0(x_s)$ the set $V \cap \varphi_0^{-1}(\{y_1, \dots, y_s\})$ is finite. We choose a linear form on $\mathbb{A}^n$, say φ_1 , distinguishing the elements of $V \cap \varphi_0^{-1}(\{y_1, \dots, y_s\}) \cup \{x_1, \dots, x_s\}$. Put $\varphi := (\varphi_0, \varphi_1)$. Then $\varphi(x_1), \dots, \varphi(x_s) \notin \overline{\varphi(V)}$.

We conclude the proof by showing $\overline{\varphi(V)} = \overline{\varphi(V)}$.

Since the composition $V \rightarrow \overline{\varphi(V)} \rightarrow \mathbb{A}^r$ is a finite morphism, so is also the morphism $V \rightarrow \overline{\varphi(V)}$, induced by φ . Hence it is surjective. So we have $\overline{\varphi(V)} = \overline{\varphi(V)}$.

The assertion $\dim \overline{\varphi(V)} = r$ is obvious.

Remark 4: Notations being the same as before, we observe the following consequence of Lemma 3: There exists a polynomial $F \in k[X_1, \dots, X_n]$ with $\deg F \leq \deg V$ vanishing on V but not on any of the $x_1, \dots, x_s$.

(For, by Lemma 2, $\overline{\varphi(V)}$ is a hypersurface of $\mathbb{A}^{r+1}$ with degree $\leq \deg V$.

Hence by Remark 2.3 $\overline{\varphi(V)}$ is the set of zeroes of a polynomial G of degree $\leq \deg V$. G doesn't vanish at $\varphi(x_1), \dots, \varphi(x_s)$.

Taking G back by φ and interpreting $X_1, \dots, X_n$ as the coordinate functions of $\mathbb{A}^n$, we obtain a polynomial $F \in k[X_1, \dots, X_n]$ as desired.)

This is used in the proof of the following proposition.

Proposition 3: Let V be an irreducible closed subset of $\mathbb{A}^n$. There exist $n+1$ polynomials $F_1, \dots, F_{n+1} \in k[X_1, \dots, X_n]$ of degree $\leq \deg V$ such that $V = \{F_1 = 0, \dots, F_{n+1} = 0\}$, i.e. such that V is the set of common zeroes of them.

Proof: We fix n and show by induction on k the slightly sharper assertion that for $1 \leq k \leq n+1$ there exist k polynomials $F_1, \dots, F_k$ of degree $\leq \deg V$ vanishing on V , such that for every component C of $\{F_1 = 0, \dots, F_k = 0\}$ the following implication holds:

$$C \not\subset V \Rightarrow \text{codim } C = k.$$

For $k = 1$ the assertion holds by Remark 4.

Let the assertion be true for k . We show it for $k+1$.

To each component C of $\{F_1 = 0, \dots, F_k = 0\}$ with $C \not\subset V$ we choose an element $x_C \in C - V$. By Remark 4 there exists some $F_{k+1} \in k[X_1, \dots, X_n]$ with $\deg F_{k+1} \leq \deg V$ vanishing on V but not at any of the x_C .

Let D be a component of $\{F_1 = 0, \dots, F_{k+1} = 0\}$ with $D \not\subset V$.

We show $\text{codim } D = k+1$, concluding thus the proof of the proposition.

There exists a component C of $\{F_1 = 0, \dots, F_k = 0\}$ containing D . Since $D \not\subset V$, we have $C \not\subset V$, whence $\text{codim } C = k$ by the induction hypothesis.

Since $x_C \in C$ but $F_{k+1}(x_C) \neq 0$, $\{F_{k+1} = 0\}$ intersects C properly.

Furthermore, D is a component of $C \cap \{F_{k+1} = 0\}$. So we have by the Dimension Theorem of algebraic geometry (Mumford), Chapter I, § 7, Theorem 2, or (Shafarevich 1972), Chapter I, § 6, Theorem 5, $\text{codim } D = k+1$ as desired.

The following theorem is a slight but useful generalization of Proposition 3.

Theorem 3: Let x be a finite set of constructible subsets of $\mathbb{A}^n$.

Then there exist polynomials $F_1, \dots, F_s \in k[X_1, \dots, X_n]$ with $\sum_{1 \leq i \leq s} \deg F_i \leq (n+1) \text{grd } x$ such that x is $(F_1, \dots, F_s)$ -definable.

Proof: Obvious by Proposition 3.

Next we are going to see how grade behaves under projection maps. The main tool for this is Theorem 3. It will serve us to investigate definability in cases where quantifiers are involved.

Assume $n \geq 1$ and let $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$ be the projection mapping each point of $\mathbb{A}^n$ on its first $n-1$ coordinates.

For simplicity consider the polynomial rings $k[X_1, \dots, X_n]$ and $k[X_1, \dots, X_{n-1}]$ in the indeterminates $X_1, \dots, X_n$ over k as the coordinate rings of $\mathbb{A}^n$ and $\mathbb{A}^{n-1}$ respectively, the inclusion map $k[X_1, \dots, X_{n-1}] \rightarrow k[X_1, \dots, X_n]$ being induced by π .

For X , a finite set of constructible subsets of $\mathbb{A}^n$ write

$$\pi(X) := \{ \pi(X) ; X \in X \}.$$

By Chevalley's Constructibility Theorem (Mumford), Chapter I, § 8, Corollary 2, the elements of $\pi(X)$ are constructible subsets of $\mathbb{A}^{n-1}$.

Our next purpose is to find a small upper bound for $\text{grd } \pi(X)$.

First we consider the case where X consists of only one single irreducible closed subset V of $\mathbb{A}^n$.

The following lemma is a quantitative version of Chevalley's Constructibility Theorem.

Lemma 4: Let V be an irreducible closed subset of $\mathbb{A}^n$. To V there exist finite sets W, W' of irreducible closed subsets of $\mathbb{A}^n$ and a map $W \rightarrow k[X_1, \dots, X_n]$ which assigns to each $W \in W$ a polynomial G_W with $W_{G_W} := \{ x \in W ; G_W(x) \neq 0 \} \neq \emptyset$ having the following properties:

$$(i) \quad V = \bigcup_{W \in W} W_{G_W} \cup \bigcup_{W' \in W'} W'.$$

(ii) For $W \in W$ the morphism $W_{G_W} \rightarrow (\overline{\pi(W)})_{G_W}$, induced by π , is finite.

For $W' \in W'$ $\pi(W')$ is a closed subset of $\mathbb{A}^{n-1}$ with $W' = \pi(W') \times \mathbb{A}^1$.

So the map $W' \rightarrow \pi(W')$, induced by π , is itself a projection map.

$$(iii) \quad \deg(\{G_W = 0\}; W \in W) \cup W \cup W') \leq n^n (\deg V)^{2n}.$$

Proof: The lemma is obvious for $n=1$. So let $n>1$.

By Proposition 3 choose $F_1, \dots, F_{n+1} \in k[X_1, \dots, X_n]$ of degree $\leq \deg V$ such that $V = \{F_1 = 0, \dots, F_{n+1} = 0\}$. Consider the F_k , $k=1, \dots, n+1$, as polynomials in X_n over $k[X_1, \dots, X_{n-1}]$. Denote by G the set of all nonzero coefficients of the F_k , except the constant terms. Let V consist of V and the $\{G=0\}$ with $G \in G$, considered as closed subsets of A^n . We have

$$(6) \quad \text{grd } V \leq \deg V \leq \deg V + \sum_{G \in G} \deg G \\ \leq \deg V + (n+1) \frac{(\deg V - 1) \deg V}{2} < n (\deg V)^2,$$

the last inequality being strict since $n>1$.

$$\text{Put } W := \{W \in C(D(V)) ; W \subset V, \exists G \in G, W \not\subset \{G=0\}\} \\ W' := \{W' \in C(D(V)) ; W' \subset V, \forall G \in G, W' \subset \{G=0\}\}.$$

To each $W \in W$ choose F_W among the $F_1, \dots, F_{n+1}$, such that there exist some coefficient of F_W not vanishing at all points of W . Among the coefficients of F_W with this property let G_W be the one belonging to the highest power of X_n . Obviously $W_{G_W} \neq \emptyset$ and, since W is contained in V , $G_W \in G$.

First we show (i).

Clearly $V \supset \bigcup_{W \in W} W_{G_W} \cup \bigcup_{W' \in W'} W'$. So, for $x \in V$ it suffices to show

$$x \in \bigcup_{W \in W} W_{G_W} \cup \bigcup_{W' \in W'} W'.$$

Let W^* be a component of $V \cap \{G=0 ; G \in G, G(x)=0\}$ which contains x .

Since $V \cap \{G=0 ; G \in G, G(x)=0\} \in D(V)$ and $W^* \subset V$ we have $W^* \in W \cup W'$.

If $W^* \in W'$ there is nothing to show.

If $W^* \in W$ we have $G_{W^*}(x) \neq 0$, since otherwise $W^* \subset \{G_{W^*}=0\}$ which is impossible by definition of G_{W^*} .

So we have in the first case $x \in W^*$ and in the second $x \in W_{G_{W^*}}$, whence

$$x \in \bigcup_{W \in W} W_{G_W} \cup \bigcup_{W' \in W'} W'.$$

Next we show (ii).

Let $W \in W$ and let ξ_n be the coordinate function of W induced by X_n . Note that $k[W] = k[\bar{W}][\xi_n]$.

The coefficients of F_W which belong to $k[X_1, \dots, X_{n-1}]$, induce functions on $\overline{\pi(W)}$. In particular the restriction of G_W on $\overline{\pi(W)}$ is a nonzero element of $k[\overline{\pi(W)}]$. So, F_W induces in $k[W]$ a nontrivial polynomial equation for ξ_n with coefficients in $k[\overline{\pi(W)}]$. The highest coefficient of this equation is the element of $k[\overline{\pi(W)}]$ coming from G_W , so ξ_n is integral over $k[(\overline{\pi(W)})_{G_W}]$. Therefore the morphism $W_{G_W} \rightarrow (\overline{\pi(W)})_{G_W}$ is finite.

To show the second assertion of (ii), let $W' \in W'$.

Since $c(D(V)) = c(Z(V))$ we have as a consequence of (5) that W' is a component of $V \cap \{G=0; G \in G\}$. On the other side, since $W' \subset V$ and since each $G \in G$ vanishes on W' , all the coefficients of $F_1, \dots, F_{n+1}$ vanish on W' .

So $F_1, \dots, F_{n+1}$ vanish on $\overline{\pi(W')} \times \mathbb{A}^1$. From this we have $\overline{\pi(W')} \times \mathbb{A}^1 \subset V$.

Furthermore we have $W' \subset \overline{\pi(W')} \times \mathbb{A}^1 \subset V \cap \{G=0; G \in G\}$.

Since $\overline{\pi(W')} \times \mathbb{A}^1$ is irreducible and W' is a component of $V \cap \{G=0; G \in G\}$, we have $W' = \overline{\pi(W')} \times \mathbb{A}^1$.

From this follows that $\overline{\pi(W')}$ is closed and $W' = \overline{\pi(W')} \times \mathbb{A}^1$.

Finally we show (iii).

Note that $(\{G_W=0\}; W \in W)$, W and W' are contained in $c(D(V))$.

Hence we have by means of Theorem 2 (i) and inequality (6)

$$\begin{aligned} \deg(\{G_W=0\}; W \in W \cup W \cup W') &\leq \deg c(D(V)) \\ &= \deg D(V) \\ &\leq (1 + \deg V)^n \\ &\leq n^n (\deg V)^{2n}. \end{aligned}$$

The core of this rather technical lemma is the following

Corollary 2: Let V be an irreducible closed subset of A^n . Then

$$\text{grd } \pi(V) \leq n^n (\deg V)^{2n}.$$

Proof: By Lemma 4 (i) and (ii) and by the surjectivity of finite morphisms (Mumford), Chapter I, § 7, Proposition 3, or (Shafarevich 1972), Chapter I, § 5, Theorem 4, we have

$$\pi(V) = \bigcup_{W \in \mathcal{W}} \pi(W_{G_W}) \cup \bigcup_{W' \in \mathcal{W}'} \pi(W') = \bigcup_{W \in \mathcal{W}} \overline{(\pi(W))}_{G_W} \cup \bigcup_{W' \in \mathcal{W}'} \pi(W'),$$

with $\overline{\pi(W')} = \pi(W')$ for $W' \in \mathcal{W}'$. Hence

$\pi(V)$ is $\gamma := \{\overline{\pi(W)}; W \in \mathcal{W} \cup \mathcal{W}'\} \cup \{G_W = 0; W \in \mathcal{W}\}$ - definable.

By Lemma 2 and Lemma 4 (iii) we have

$$\text{grd } \{\pi(V)\} \leq \deg \gamma \leq n^n (\deg V)^{2n}.$$

We are going to investigate the situation where besides from V an additional polynomial $F \in k[X_1, \dots, X_n]$ with $\deg F > 0$ is given, and we want to find a bound for $\text{grd } \{\pi(V_F)\}$.

For the moment consider instead of V an irreducible closed subset W of A^n which later will be chosen from $\mathcal{W}$ of Lemma 4.

Denote by $\xi_1, \dots, \xi_n$ the coordinate functions of W induced by $X_1, \dots, X_n$ and by φ the function induced by F on W .

Let T be a new indeterminate. Consider the kernel p of the ring homomorphism $k[X_1, \dots, X_{n-1}, T] \rightarrow k[\xi_1, \dots, \xi_{n-1}, \varphi] = k[\overline{\pi(W)}][\varphi]$, mapping $X_1, \dots, X_{n-1}$ on $\xi_1, \dots, \xi_{n-1}$ and T on φ . Roughly speaking, p describes the equations satisfied by φ over $k[\overline{\pi(W)}]$.

Lemma 5: The set of zeroes of p has degree $\leq \deg W \cdot \deg F$, and consequently p is the radical of an ideal spanned by $n+1$ polynomials of $k[X_1, \dots, X_{n-1}, T]$ each of degree $\leq \deg W \cdot \deg F$.

Proof: Consider the image W^* of W under the morphism $\mathbb{A}^n \rightarrow \mathbb{A}^{n+1}$, which maps $(x_1, \dots, x_n) \in \mathbb{A}^n$ on $(x_1, \dots, x_n, F(x_1, \dots, x_n)) \in \mathbb{A}^{n+1}$. Since $W^* = (W \times \mathbb{A}^1) \cap \{F(X_1, \dots, X_n) - T = 0\}$ we have by Theorem 1 $\deg W^* \leq \deg W \cdot \deg F$. The set of zeroes of p is the closure of the image of W^* under the morphism $\mathbb{A}^{n+1} \rightarrow \mathbb{A}^n$ mapping $(x_1, \dots, x_n, F(x_1, \dots, x_n)) \in \mathbb{A}^{n+1}$ on $(x_1, \dots, x_{n-1}, F(x_1, \dots, x_n)) \in \mathbb{A}^n$, whence Lemma 5 by Lemma 2 and Theorem 3.

Now let $H_1, \dots, H_s \in k[X_1, \dots, X_{n-1}, T]$ be such that the radical of the ideal spanned by them is p . We consider the H_k , $k=1, \dots, s$, as polynomials in T over $k[X_1, \dots, X_{n-1}]$.

Denote by H the set of the coefficients of the H_k . H consists of elements of $k[X_1, \dots, X_{n-1}]$.

Lemma 6: Let $G \in k[X_1, \dots, X_{n-1}]$ be such that $W_G \neq \emptyset$ and such that the morphism $W_G \rightarrow (\overline{\pi(W)})_G$, induced by $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$ is finite. Then the ideal spanned by H doesn't vanish at any point of $(\overline{\pi(W)})_G$.

Proof: Note that $k[(\overline{\pi(W)})_G][\varphi]$ is contained in $k[W_G]$. Hence, by the finiteness of $W_G \rightarrow (\overline{\pi(W)})_G$, the ring extension $k[(\overline{\pi(W)})_G] \subset k[(\overline{\pi(W)})_G][\varphi]$ is integral. To $k[(\overline{\pi(W)})_G] \subset k[(\overline{\pi(W)})_G][\varphi]$ there corresponds a finite morphism, say ψ , of the local closed affine subvariety $\{H_1 = 0, \dots, H_s = 0\}_G$ of $\mathbb{A}^n$ onto $(\overline{\pi(W)})_G$.

If the ideal spanned by H would vanish at some point $y \in (\overline{\pi(W)})_G$, the polynomials $H_1(y, T), \dots, H_s(y, T)$ would vanish identically. Since $G(y) \neq 0$ y would then have an infinite fibre $\psi^{-1}(y)$ contradicting the finiteness of ψ . (Compare (Mumford), Chapter I, § 7, Proposition 3, (Shafarevich 1972) Chapter I, § 5.3.)

We summarize this series of technical lemmas by the following proposition:

Proposition 4: Let V be an irreducible closed subset of A^n and $F \in k[X_1, \dots, X_n]$ with $\deg F > 0$. Then we have for $V_F := \{x \in V; F(x) \neq 0\}$

$$\text{grd}(\pi(V_F)) \leq n^{2n^2 + 3n} (\deg V)^{4n^2} \cdot (\deg F)^{2n}.$$

Proof: For simplicity let notations be the same as in the foregoing lemmas.

The proposition is obvious for $n=1$. So let $n > 1$.

As we have seen in Lemma 5, for $W \in \mathcal{W}$ the equations over $k[\overline{W}]$ satisfied by the restriction of F on W give rise to a prime ideal of $k[X_1, \dots, X_{n-1}, T]$, which is the radical of an ideal spanned by $n+1$ polynomials of

$k[X_1, \dots, X_{n-1}, T]$, say $H_1^W, \dots, H_{n+1}^W$, each of degree $\leq \deg W \cdot \deg F$.

Let H^W be the set of coefficients of the H_k^W , $k=1, \dots, n+1$, considered as polynomials in T over $k[X_1, \dots, X_n]$.

Let U be the union of $W \cup W'$ with the set of all $\{L=0\}$, where L is a coefficient of F , (F being considered as a polynomial in X_n over $k[X_1, \dots, X_{n-1}]$), or $L = G_W$ or $L \in H^W$ for some $W \in \mathcal{W}$.

Since $n > 1$ we have by Lemma 4 (iii)

$$\begin{aligned} \text{grd } U &\leq \deg(\{(G_W=0); W \in \mathcal{W}\} \cup W \cup W') + (\deg F)^2 + (n+1) \sum_{W \in \mathcal{W}} (\deg W \cdot \deg F)^2 < \\ &< n^{2n+3} (\deg V)^{4n} \cdot (\deg F)^2. \end{aligned}$$

Let $\mathcal{W}^* := C(D(U))$ and $\mathcal{Y} := \{\overline{\pi(C)}; C \in \mathcal{W}^*\}$. $\mathcal{Y}$ is a finite set of irreducible closed subsets of A^{n-1} . Then by Lemma 2 and Theorem 2 we have

$$\deg \mathcal{Y} \leq \deg \mathcal{W}^* \leq (1 + \text{grd } U)^n \leq n^{2n^2 + 3n} (\deg V)^{4n^2} \cdot (\deg F)^{2n}.$$

We show that $\pi(V_F)$ is $\mathcal{Y}$ -definable. This implies the proposition.

Let $y \in \pi(V_F)$. We have to find a $\mathcal{Y}$ -definable subset Y of A^{n-1} such that $y \in Y \subset \pi(V_F)$. Choose $x \in V_F$ such that $y = \pi(x)$.

First consider the case where x is contained in some $W' \in W'$.

Since $F(x) \neq 0$ there is a coefficient L of F (F being considered as a polynomial in X_n over $k[X_1, \dots, X_{n-1}]$), such that $L(y) \neq 0$.

By Lemma 4 (ii), $\pi(W')$ is an irreducible closed subset of A^{n-1} and W' is a cylindrical set, namely $W' = \pi(W') \times A^1$. So we have $y \in \pi(W')_L \subset \pi(W'_F) \subset \pi(V_F)$ and $\pi(W') \in Y$.

We put $Y := \pi(W')_L$. Y is obviously Y -definable.

Now we consider the case where $x \in W_{G_W}$ for some $W \in W$.

Let C be a component of $W \cap \{L=0; L \in H^W, L(y) \neq 0\}$ which contains x .

Obviously we have $C \in W^*$. Clearly $x \in C_{G_W} \subset W_{G_W}$.

Since $F(x) \neq 0$, F induces a nonzero element, say φ , of $k[C]$.

By Lemma 6 there is a $L \in H^W$ such that $L(y) \neq 0$. Hence one of the H_k^W induces a nontrivial polynomial equation for φ on C , say

$$(7) \quad \lambda_t \varphi^t + \dots + \lambda_0 = 0 \quad \text{with } \lambda_t, \dots, \lambda_0 \in k[\overline{\pi(C)}].$$

Dividing the equation by a suitable power of φ , if necessary, we can assume

$\lambda_0 \neq 0$ in (7). But since by the choice of C , $\lambda_0(y) = 0$ would imply $\lambda_0 = 0$ we have $\lambda_0(y) \neq 0$. To simplify notations we assume that λ_0 is induced by L . So, by (7), F doesn't vanish at points of C at which L doesn't.

Note that x is contained in $C_{G_W \cdot L}$ which is mapped finitely onto $(\overline{\pi(C)})_{G_W \cdot L}$ by π . So we have

$$Y \in (\overline{\pi(C)})_{G_W \cdot L} = \pi(C_{G_W \cdot L}) \subset \pi(C_{G_W \cdot F}) \subset \pi(W_{G_W \cdot F}) \subset \pi(V_F).$$

We choose $Y := (\overline{\pi(C)})_{G_W \cdot L}$. Since $C \in W^*$ we have $\overline{\pi(C)} \in Y$. So, as in the previous case, Y is Y -definable. By Lemma 4 (i) we conclude that $\pi(V_F)$ is Y -definable, which finishes the proof.

The following theorem is a straightforward consequence of Proposition 4 :

Theorem 4: There exists a constant $c > 0$ such that for any finite set X of constructible subsets of $\mathbb{A}^n$

$$\text{grd } \pi(X) \leq (n \text{ grd } X)^c n^3$$

holds.

Proof: The case $n=1$ is obvious. So let $n > 1$.

By Theorem 3 choose polynomials $F_1, \dots, F_s \in k[X_1, \dots, X_n]$, none of them constant, with $\sum_{1 \leq k \leq s} \deg F_k \leq (n+1) \text{ grd } X$, such that the elements of X are $F_1, \dots, F_s$ -definable. Let Z be the set of $(F_1, \dots, F_s)$ -cells of $\mathbb{A}^n$. Note that the elements of $\pi(X)$ are $\pi(Z)$ -definable.

By Corollary 1 of Theorem 2 note further $\# Z \leq (1 + (n+1) \text{ grd } X)^n$.

Let $Z \in Z$ be a cell defined by $Z := \bigcap_{k \in I} \{F_k = 0\} \cap \bigcap_{\ell \in \{1, \dots, s\} - I} (\mathbb{A}^n - \{F_\ell = 0\})$

for some $I \subset \{1, \dots, s\}$ and write $F := \bigcap_{\ell \in \{1, \dots, s\} - I} F_\ell$.

Then $Z = \bigcup_{C \in C(\{Z\})} C_F$, $\deg F \leq (n+1) \text{ grd } X$, and, by Corollary 1 of

Theorem 2, $\deg Z \leq (1 + (n+1) \text{ grd } X)^n$.

For $C \in C(\{Z\})$ we have by Proposition 4

$$\text{grd } \{\pi(C_F)\} \leq n^2 n^2 + 3n (\deg C)^{4n^2} \cdot (\deg F)^{2n}, \text{ hence}$$

$$\begin{aligned} \text{grd } \{\pi(Z)\} &\leq \sum_{C \in C(\{Z\})} \text{grd } \{\pi(C_F)\} \leq n^2 n^2 + 3n (\deg Z)^{4n^2} \cdot (\deg F)^{2n} \leq \\ &\leq n^2 n^2 + 3n (n+1)^{2n} (\text{grd } X)^{2n} (1 + (n+1) \text{ grd } X)^{4n^3}. \end{aligned}$$

Finally we obtain

$$\begin{aligned} \text{grd } \pi(Z) &\leq \sum_{Z \in Z} \text{grd } \{\pi(Z)\} \leq \\ &\leq n^2 n^2 + 3n (n+1)^{2n} (\text{grd } X)^{2n} (1 + (n+1) \text{ grd } X)^{4n^3 + n} \leq \\ &\leq (n \text{ grd } X)^{cn^3} \quad \text{for suitable chosen } c > 0. \end{aligned}$$

Now the theorem follows by $\text{grd } \pi(X) \leq \text{grd } \pi(Z)$.

Now we are ready to investigate definability in cases where quantifiers are involved.

Let X be a finite set of constructible subsets of $\mathbb{A}^n$. We define $D_m(X)$ inductively as follows:

$$D_0(X) := D(X)$$

$D_{m+1}(X) :=$ the boolean algebra generated by the images of $D_m(X)$ under the projection $\mathbb{A}^{n-m} \rightarrow \mathbb{A}^{n-m-1}$ which maps each point of $\mathbb{A}^{n-m}$ on its first $n-m-1$ coordinates.

Note that by Chevalley's Constructibility Theorem (Mumford), Chapter I, § 8, Corollary 2, the elements of $D_m(X)$ are constructible subsets of $\mathbb{A}^{n-m}$.

We call the elements of $D_m(X)$ X -definable with m quantifiers.

This is justified by the following reason: consider the elements of X as defined by n -place predicates $P_1(X_1, \dots, X_n), \dots, P_s(X_1, \dots, X_n)$ in the variables $X_1, \dots, X_n$ which correspond to the coordinates of $\mathbb{A}^n$. Then any prenex first order formula in the $n-m$ free variables $X_1, \dots, X_{n-m}$ built up from $P_1(X_1, \dots, X_n), \dots, P_s(X_1, \dots, X_n)$ using m quantifiers defines an element of $D_m(X)$. However, the converse is not true.

There is a rather interesting case, namely, when the quantifiers in the defining formula all are existential.

To be precise: we call a subset of $\mathbb{A}^{n-m}$ X -definable with m existential quantifiers if it is the image of a X -definable subset of $\mathbb{A}^n$ under the projection $\mathbb{A}^n \rightarrow \mathbb{A}^{n-m}$ mapping each point of $\mathbb{A}^n$ on its first $n-m$ coordinates.

As an immediate consequence of Theorem 2 we have the following proposition.

Proposition 5: Let X be a finite set of constructible subsets of $\mathbb{A}^n$. A finite subset of $\mathbb{A}^{n-m}$ which is X -definable with existential quantifiers contains at most $(1 + \text{grd } X)^n$ points.

The number of subsets of $\mathbb{A}^{n-m}$ which are X -definable with m existential quantifiers doesn't exceed $2^{(1 + \text{grd } X)^n}$.

Proof: The elements of any finite subset of $\mathbb{A}^{n-m}$ which is X -definable with m existential quantifiers are images of elements of $C(\mathcal{D}(X))$ under the projection map $\mathbb{A}^n \rightarrow \mathbb{A}^{n-m}$. So, by Theorem 2 (i), their number can't exceed $(1 + \text{grd } X)^n$.

The second assertion of the proposition follows directly from Theorem 2 (iv).

The main bound of Theorem 2 and this proposition can be summarized as being polynomial in $\text{grd } X$ and exponential in n , the number of variables. The number m of bounded variables doesn't appear explicitly in the estimates of Proposition 5.

In the general case of X -definability with m quantifiers our estimate will be polynomial in $\text{grd } X$, exponential in n , and double exponential in m .

Theorem 4 provides us with the key bound for X -definability with one quantifier. We will generalize this result on X -definability with several quantifiers.

Theorem 5: Let X be a finite set of constructible subsets of $\mathbb{A}^n$ with $n > 1$. There exists a constant $c > 0$ such that

$$\text{grd } D_m(X) \leq n^{(cn^6)^m} (\text{grd } X)^{(cn^3)^m}.$$

Proof: Choose $c \geq 2$ such that the inequality in Theorem 4 holds with $\sqrt{c}$ as constant. We show Theorem 5 with this constant c by induction on n .

Since $\text{grd } D_0(X) = \text{grd } X$, this is trivial for $m=0$.

Now we assume the inequality for m and show it for $m+1$. Let π be the projection $\pi: \mathbb{A}^{n-m} \rightarrow \mathbb{A}^{n-m-1}$. By Theorem 4 and the induction hypothesis we obtain

$$\begin{aligned} \text{grd } D_{m+1}(X) &= \text{grd } \pi(D_m(X)) \leq (n \text{grd } D_m(X))^{\sqrt{c}} n^3 && \leq \\ &\leq n^{c^m \sqrt{c} n^{6m+3} + \sqrt{c} n^3} (\text{grd } X)^{c^m \sqrt{c} n^{3m+3}} && \leq \\ &\leq n^{(cn^6)^{m+1}} (\text{grd } X)^{(cn^3)^{m+1}}. \end{aligned}$$

Corollary 3: Let X be a finite set of constructible subsets of $\mathbb{A}^n$ with $n \geq 1$. There exists a constant $c > 0$ such that

- (i) $\deg D_m(X) \leq n^m n^{6m+1} (\text{grd } X)^m n^{3m+1}$. Consequently, a finite subset of $\mathbb{A}^{n-m}$ which is X -definable with m quantifiers contains at most $n^m n^{6m+1} (\text{grd } X)^m n^{3m+1}$ points.
- (ii) $D_m(X) \leq 2^n n^m n^{6m+1} (\text{grd } X)^m n^{3m+1}$.

Proof: The case $n=1$ is obvious. For $n > 1$ choose c integer and sufficiently large such that in Theorem 5 the strict inequality holds. Then the corollary follows by Theorem 2.

Note that for $m=0$ the bounds of Corollary 3 are slightly worse than those of Theorem 2, the "defect" stemming mainly from the fact that the proof of Theorem 5 is based on Theorem 3.

To conclude, we give a partial version of Corollary 3 in a down-to-earth form :

Corollary 4: There exists a constant $c > 0$ with the following property : Let $F_1, \dots, F_S \in k[X_1, \dots, X_n]$ be polynomials in the indeterminates $X_1, \dots, X_n$ over k , $d := \sum_{1 \leq k \leq S} \deg F_k$ and $0 \leq m \leq n$.

Any finite subset of $\mathbb{A}^{n-m}$ definable by a prenex first order formula built up by the $F_1, \dots, F_S$, using m quantifiers, contains at most

$$n^m n^{6m+1} d^m n^{3m+1} \text{ points.}$$

The number of all subsets of $\mathbb{A}^{n-m}$ definable in this way doesn't exceed

$$2^n n^m n^{6m+1} d^m n^{3m+1}.$$

III . Quantifier Elimination

In the sequel, assertions which contain constants (denoted by $c, c_1, c_2, \dots$) have to be read as "there is a constant $c > 0$ such that..." , although this rather complicated formulation is not given explicitly every time.
 "Turing - Machine" has to be understood as 1-tape deterministic Turing-Machine.
 log means logarithm to the basis 2.

Let R be one of the rings $\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \dots, \mathbb{Z}_p, \dots$ where p is any prime number.

Let $\sigma : R \rightarrow [1, \infty)$ be defined as follows :

in the case $R = \mathbb{Z}$ $\sigma(z) := \lceil \log |z| \rceil$

and in the case $R = \mathbb{Z}_p$ $\sigma(z) := \lceil \log p \rceil$, $z \in R$.

Let $X_1, \dots, X_n$ be indeterminates over R .

For $F \in R[X_1, \dots, X_n]$ with $F = \sum f_{i_1, \dots, i_n} X_1^{i_1} \dots X_n^{i_n}$, $f_{i_1, \dots, i_n} \in R$ we put

$$\sigma(F) := \max \{ 1 + \deg F \} \cup \{ \sigma(f_{i_1, \dots, i_n}) ; i_1, \dots, i_n \}$$

Extending thus σ on $R[X_1, \dots, X_n]$ we have the following inequalities for σ :

Let $F, F_1, \dots, F_s \in R[X_1, \dots, X_n]$ with $v = \max_{1 \leq i \leq s} (\sigma(F_i))$. Then

$$(8) \quad \sigma(F) = \sigma(-F)$$

$$(9) \quad \sigma\left(\sum_{1 \leq i \leq s} F_i\right) \leq v + \log s$$

$$(10) \quad \sigma\left(\prod_{1 \leq i \leq s} F_i\right) \leq (n+1) s v$$

For $s = 2$, if F_2 divides F_1 we have

$$(11) \quad \sigma(F_1/F_2) \leq v^{2n+1}$$

σ measures the length of n -variate polynomials by some straightforward encoding of them on a Turing - Machine tape.

Under such an encoding the complexity function L , which measures the costs to perform addition/subtraction, multiplication and division (if possible in $R[X_1, \dots, X_n]$) on a Turing-Machine, behaves as follows

($L(F; F_1, \dots, F_s)$ denotes the minimal time to compute F when $F_1, \dots, F_s$ are given as input) :

$$(12) \quad L\left(\sum_{1 \leq i \leq s} F_i ; F_1, \dots, F_s\right) \leq c s v^{(n+1)}$$

$$(13) \quad L\left(\prod_{1 \leq i \leq s} F_i ; F_1, \dots, F_s\right) \leq c (sv)^{C(n+1)}$$

and, for $s=2$, if F_2 divides F_1 we have

$$(14) \quad L(F_1/F_2; F_1, F_2) \leq c v^{c(n+1)}.$$

Let q and r be natural numbers. For $q \times r$ -matrices $M = (F_{kl})$ with $F_{kl} \in R[X_1, \dots, X_n]$ we define

$$\sigma(M) := \max_{k,l} (\sigma(F_{kl})).$$

Then, for $q = r$, we have

$$(15) \quad \sigma(\det M) \leq c(n+1) q^2 \sigma(M),$$

$$(16) \quad L(\det M; M) \leq (q \sigma(M))^{c(n+1)}.$$

All inequalities except (11), (14), and (16) are straightforward. For (11) and (14) we consider the coefficients of $F := F_1/F_2$ as solutions of the system of linear equations given by $F_2 \cdot F = F_1$ comparing coefficients. Then by Cramer's rule we get (11), and by Lemma 7 we will see that some modified Gauss-elimination can be performed in R . So we get (14) and similarly (16). For $n = 0$ we obtain the corresponding inequalities for R .

Remark 5: Everything that will be said in the sequel about R , being one of the rings $\mathbb{Z}, \mathbb{Z}_2, \dots, \mathbb{Z}_p, \dots$, holds for any ring R whose elements can be encoded on a Turing-Machine tape such that (8) - (16) are satisfied.

The results remain also valid for the computing model which counts only arithmetical operations in R . In this case $\sigma(z) := 1$ for $z \in R$ and consequently $\sigma(F) := 1 + \deg F$ for $F \in R[X_1, \dots, X_n]$.

Now we consider $q \times r$ -systems of inhomogeneous linear equations over $R[X_1, \dots, X_n]$ in the unknowns $T_1, \dots, T_r$:

$$(17) \quad \begin{array}{l} F_{11} T_1 + \dots + F_{1r} T_r = F_{1r+1} \\ \vdots \\ F_{q1} T_1 + \dots + F_{qr} T_r = F_{qr+1} \end{array}, \quad F_{kl} \in R[X_1, \dots, X_n].$$

We represent (17) by

$$M = \begin{pmatrix} F_{11} & \dots & F_{1r} & F_{1r+1} \\ \vdots & & \vdots & \vdots \\ F_{q1} & \dots & F_{qr} & F_{qr+1} \end{pmatrix} \quad \text{and call} \quad \begin{pmatrix} F_{11} & \dots & F_{1r} \\ \vdots & & \vdots \\ F_{q1} & \dots & F_{qr} \end{pmatrix} \quad \text{the matrix}$$

$$\text{and} \quad \begin{pmatrix} F_{1r+1} \\ \vdots \\ F_{qr+1} \end{pmatrix} \quad \text{the inhomogeneous part of the system.}$$

A Gauss - algorithm in $R[X_1, \dots, X_n]$ is a sequence of $q \times r$ -systems of inhomogeneous linear equations

$$M_1 = (F_{kl}^{(1)}) \dots, M_i = (F_{kl}^{(i)}) \dots, M_s = (F_{kl}^{(s)})$$

over $R[X_1, \dots, X_n]$ such that for each $1 \leq i < s-1$ $F_{ii}^{(i+1)} \neq 0$ and such that M_{i+1} is constructed from M_i in the following way :

there is a matrix $N = (G_{kl})$ obtained from M_i by interchanging only rows of index $k \geq i$ and columns of index $i \leq l \leq r$ such that

$$F_{kl}^{(i+1)} = \begin{cases} G_{kl} & \text{for } k \leq i \text{ or } l < i \\ \det \begin{pmatrix} G_{ii} & G_{il} \\ G_{ki} & G_{kl} \end{pmatrix} / G_{i-1 i-1} & \text{for } k > i \text{ or } l \geq i \end{cases}$$

(for $i=1$ we put $G_{00} = 1$).

Note that this definition makes sense since $G_{i-1 i-1} = F_{i-1 i-1}^{(i)} \neq 0$ for $1 < i \leq s-1$

We call 1 the 0-th and $F_{ii}^{(i+1)}$, $1 \leq i \leq s-1$, the i -th pivot of the Gauss - algorithm. The algorithm is essentially determined by the choice of its pivots.

The following lemma shows that our definition of Gauss - algorithm differs only slightly from what is generally meant by Gaussian elimination.

Let $M = (F_{kl})$ be a $q \times r$ -system of inhomogeneous linear equations over $R[X_1, \dots, X_n]$. With the same notations as before we have

Lemma 7 (Bareiss 1968, Edmonds 1967) : Let $M = M_1, \dots, M_s$ be a Gauss - algorithm. If $F_{s-1 s-1}^{(s)} \neq 0$ then $F_{s-1 s-1}^{(s)}$ divides $\det \begin{pmatrix} F_{ss}^{(s)} & F_{sl}^{(s)} \\ F_{ks}^{(s)} & F_{kl}^{(s)} \end{pmatrix}$ for each $k > s$ and $l \geq s$. Moreover, if no row and columns have been interchanged during the algorithm, we have

$$(18) \quad F_{kl}^{(s)} = \det \begin{pmatrix} F_{11} \dots F_{1s} & F_{1l} \\ F_{s1} \dots F_{ss} & F_{sl} \\ F_{k1} \dots F_{ks} & F_{kl} \end{pmatrix}$$

Proof : The basic idea of the lemma is the following remark :

Let $A = (A_{hj})$ be a $t \times t$ -matrix with entries in $R[X_1, \dots, X_n]$, $t > 1$; $A_{11} \neq 0$. Then

$$(19) \quad \det \left(\det \begin{pmatrix} A_{11} & A_{1j} \\ A_{h1} & A_{hj} \end{pmatrix} \right)_{1 < h, j} = A_{11}^{t-2} \cdot \det A \quad .$$

The proof works now by induction on s .

For the sake of notational simplicity, we assume that no rows and columns are interchanged in the Gauss - algorithm, and we slightly generalize the notion of

Gauss-algorithm, admitting any 0-th pivot $F_{00} \neq 0$ such that F_{00}^{i-1} divides the determinants of all $i \times i$ -submatrices of M .

Under this hypothesis, the first assertion we want to prove remains the same, whereas (18) changes into

$$(20) \quad F_{00}^s \cdot F_{kl}^{(s)} = \det \begin{pmatrix} F_{11} & \dots & F_{1s} & F_{1l} \\ \vdots & & \vdots & \vdots \\ F_{s1} & \dots & F_{ss} & F_{sl} \\ F_{k1} & \dots & F_{ks} & F_{kl} \end{pmatrix}.$$

For $s=0$ and $s=1$ there is nothing to show.

Let $s > 1$. Since no rows and columns are interchanged in the algorithm, we have $F_{11} \neq 0$.

By (19) we see that F_{11}^{i-1} divides all $i \times i$ -submatrices of

$$(F_{kl}^{(2)})_{k,l > 1} = \left[\det \begin{pmatrix} F_{11} & F_{1l} \\ F_{k1} & F_{kl} \end{pmatrix} / F_{00} \right]_{k,l > 1}.$$

Now consider the Gauss-algorithm given by

$(F_{kl}^{(2)})_{k,l > 1}, \dots, (F_{kl}^{(i+1)})_{k,l > 1}, \dots, (F_{kl}^{(s)})_{k,l > 1}$ with F_{11} as the 0-th pivot.

By the induction hypothesis if $F_{s-1,s-1}^{(s)} \neq 0$

$$F_{s-1,s-1}^{(s)} \text{ divides } \det \begin{pmatrix} F_{ss}^{(s)} & F_{sl}^{(s)} \\ F_{ks}^{(s)} & F_{kl}^{(s)} \end{pmatrix} \text{ for } k > s \text{ and } l \geq s,$$

so the first assertion of the lemma is shown.

Furthermore, we have by induction hypothesis and (19)

$$F_{11}^{s-1} \cdot F_{kl}^{(s)} = \det \begin{pmatrix} F_{22}^{(2)} & \dots & F_{2s}^{(2)} & F_{2l}^{(2)} \\ \vdots & & \vdots & \vdots \\ F_{s2}^{(2)} & \dots & F_{ss}^{(2)} & F_{sl}^{(2)} \\ F_{k2}^{(2)} & \dots & F_{ks}^{(2)} & F_{kl}^{(2)} \end{pmatrix} = \frac{F_{11}^{s-1}}{F_{00}^s} \cdot \det \begin{pmatrix} F_{11} & \dots & F_{1s} & F_{1l} \\ \vdots & & \vdots & \vdots \\ F_{s1} & \dots & F_{ss} & F_{sl} \\ F_{k1} & \dots & F_{ks} & F_{kl} \end{pmatrix}$$

for $k > s$ and $l \geq s$, whence (18).

Lemma 7 says that, similar to "normal" Gaussian elimination, Gauss-algorithms can be performed within $R[X_1, \dots, X_n]$ at any instance, provided one only chooses pivots different from zero.

We look at Gauss-algorithms as computations in $R[X_1, \dots, X_n]$ involving additions/subtractions, multiplications/divisions executed on a Turing-Machine tape.

Remark 6: As a consequence of (18) and (15) we have that the length σ of the elements of $R[X_1, \dots, X_n]$ computed by the Gauss-algorithm $M = M_1, \dots, M_s$ doesn't exceed $c(n+1)s^2\sigma(M)$, and that the whole computation can be done in $q r (s \sigma(M))^{c(n+1)}$ steps on a Turing-Machine.

Corollary 5: Let $M = (F_{kl})$, $F_{kl} \in R[X_1, \dots, X_n]$, a $q \times r$ -system of inhomogeneous linear equations. An equivalent upper-triangular $q \times r$ -system of inhomogeneous linear equations $\bar{M}$ can be computed in $R[X_1, \dots, X_n]$ performing $r(q\sigma(M))^{c(n+1)}$ steps on a Turing-Machine.

(Here equivalence means that M and $\bar{M}$ have the same solution in $K(X_1, \dots, X_n)^r$, where K denotes the field of fractions of R . Upper-triangular means that for $\bar{M} = (\bar{F}_{kl})$ $\bar{F}_{kl} = 0$ holds for $k > l$.)

Proof: Analogously to Gaussian elimination triangularize M by any Gauss-algorithm.

In the same way it can be seen easily that (16) is a consequence of (18), and (14) a consequence of Corollary 5.

In the sequel we need the following

Lemma 8 (Hermann 1928, Seidenberg 1974): Let notations be as before. Let K be the field of fractions of R , and let $M = (F_{kl})$ represent a $q \times r$ -system of inhomogeneous linear equations over $R[X_1, \dots, X_n]$. If M is solvable over $K[X_1, \dots, X_n]$, then there exists a solution $(Z_1, \dots, Z_r)$ of M with $Z_\ell \in K[X_1, \dots, X_n]$ and $\deg Z_\ell \leq (c q \sigma(M))^{3^n}$, $1 \leq \ell \leq r$.

Proof: During the proof let k be any infinite field containing K . We show the existence of a function $f: \mathbb{N}^3 \rightarrow [0, \infty)$ with

with $f(q, d, 0) = 0$ and

for $n > 0$ $f(q, d, n) \leq f(c_2 q^2 d, q d, n-1) + c_1 q^2 d$

with the following property: if the system of inhomogeneous linear equations M is solvable over $k[X_1, \dots, X_n]$, there exists a solution $(Z_1, \dots, Z_r)$, $Z_\ell \in k[X_1, \dots, X_n]$ with $\deg Z_\ell \leq f(q, d, n)$, $1 \leq \ell \leq r$, where $d := \sigma(M)$. (f doesn't depend on r .)

$f(q, d, n) \leq (c q d)^{3^n}$ follows by induction on n .

The solvability of M over $k[X_1, \dots, X_n]$ implies the solvability of M over $K[X_1, \dots, X_n]$ with the same degree bounds for the solution, since, by comparing coefficients, the solvability of M can be considered as the problem to solve some system of inhomogeneous linear equations with coefficients from R .

But solvability over k of such a system of linear equations is equivalent to its solvability over K , which implies the assertion of Lemma 8.

Without loss of generality, we may assume $q \leq r$ (reducing the number of equations, if necessary). Let $d := \sigma(M)$. Triangulizing M as described in Corollary 5, we may assume without loss of generality that M has the form

$$\begin{pmatrix} F_{11} & \cdots & F_{1q} & \cdots & F_{1r} & F_{1r+1} \\ & \ddots & \vdots & & \vdots & \vdots \\ 0 & & F_{qq} & \cdots & F_{qr} & F_{qr+1} \end{pmatrix}$$

with $\deg F_k \leq qd$ and $D = F_{11} \cdots F_{qq} \neq 0$.

We assume that M has a solution $(\bar{Y}_1, \dots, \bar{Y}_r) \in k[X_1, \dots, X_n]^r$.

Our purpose is to substitute $\bar{Y}_{q+1}, \dots, \bar{Y}_r$ by some $Y_{q+1}, \dots, Y_r \in k[X_1, \dots, X_n]$ with bounded degree in X_n .

The column vectors $M^{(\ell)} := \begin{pmatrix} F_{1\ell} \\ \vdots \\ F_{q\ell} \end{pmatrix}$, $q < \ell \leq r$ are linearly dependent on

$$M^{(1)} = \begin{pmatrix} F_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, M^{(q)} = \begin{pmatrix} F_{1q} \\ \vdots \\ F_{qq} \end{pmatrix}.$$

By Cramer's rule, we only need division by D , the non-vanishing determinant

of $\begin{pmatrix} F_{11} & \cdots & F_{1q} \\ & \ddots & \vdots \\ 0 & & F_{qq} \end{pmatrix}$, in order to represent $M^{(\ell)}$ as a linear combination

of $M^{(1)}, \dots, M^{(q)}$.

More precisely, there are $A_{k\ell} \in R[X_1, \dots, X_n]$, $1 \leq k \leq q$, $q < \ell \leq r$, such that

$$(21) \quad D \cdot F_{k\ell} = A_{k\ell} F_{kk} + \dots + A_{q\ell} F_{qq}.$$

Without loss of generality, we may assume $D = c X_n^{\deg D} + \dots \in k[X_1, \dots, X_n]$, $c \neq 0$, with $\deg D \leq q^2 d$.

(Since k is infinite, we can achieve this form of D by linear substitution of variables in $k[X_1, \dots, X_n]$.)

Division with remainder in $k[X_1, \dots, X_n]$ of $\bar{Y}_{q+1}, \dots, \bar{Y}_r$ by D gives

$$(22) \quad \bar{Y}_\ell = Q_\ell D + Y_\ell \quad \text{where} \quad q < \ell \leq r$$

and $Q_\ell, Y_\ell \in k[X_1, \dots, X_n]$, $\deg_{X_n} Y_\ell < \deg D \leq q^2 d$. (This is possible due to the special form of D .)

Substituting the equations (22) in

$$\begin{array}{ccccccc} F_{11} \bar{Y}_1 + \dots + F_{1q} \bar{Y}_q + \dots + F_{1r} \bar{Y}_r & = & F_{1r+1} \\ \vdots & & \vdots \\ F_{qq} \bar{Y}_q + \dots + F_{qr} \bar{Y}_r & = & F_{qr+1} \end{array}$$

we obtain after suitable reordering

$$(23) \quad \begin{aligned} & F_{kk} \bar{Y}_k + \dots + F_{kq} \bar{Y}_q + D F_{kq+1} Q_{q+1} + \dots + D F_{kr} Q_r + \\ & + F_{kq+1} Y_{q+1} + \dots + F_{kr} Y_r = F_{kr+1} \end{aligned} \quad , \quad 1 \leq k \leq q .$$

Using (21), we obtain from (23)

$$\begin{aligned} & F_{kk} (\bar{Y}_k + \sum_{q < \ell \leq r} A_{k\ell} Q_\ell) + \dots + F_{kq} (\bar{Y}_q + \sum_{q < \ell \leq r} A_{q\ell} Q_\ell) + \\ & + \sum_{q < \ell \leq r} F_{k\ell} Y_\ell = F_{kr+1} \end{aligned} \quad , \quad 1 \leq k \leq q .$$

We put

$$Y_1 := \bar{Y}_1 + \sum_{q < \ell \leq r} A_{1\ell} Q_\ell, \dots, Y_q := \bar{Y}_q + \sum_{q < \ell \leq r} A_{q\ell} Q_\ell .$$

Because of $\deg_{X_n} F_{k\ell} Y_\ell \leq qd + q^2 d \leq c_1(q^2 d)$ for $q < \ell \leq r$, and by the triangular form of M , we conclude

$$\deg_{X_n} Y_1, \dots, \deg_{X_n} Y_q \leq c_1(q^2 d) .$$

Thus we have shown that, if M has a solution in $k[X_1, \dots, X_n]^r$, it has also a solution $(Y_1, \dots, Y_r) \in k[X_1, \dots, X_n]^r$ with $\deg_{X_n} Y_\ell \leq c_1(q^2 d)$, $1 \leq \ell \leq r$.

We write

$$Y_\ell = \sum_{0 \leq m \leq c_1(q^2 d)} Y_{\ell m}^* X_n^m \quad \text{with} \quad Y_{\ell m}^* \in k[X_1, \dots, X_{n-1}]$$

and

$$F_{k\ell} = \sum_{0 \leq m \leq c_1(q^2 d)} F_{k\ell m}^* X_n^m, \quad F_{k\ell m}^* \in R[X_1, \dots, X_{n-1}]$$

for $1 \leq \ell \leq r$, $1 \leq k \leq q$.

Comparing coefficients of X_n , we see $(Y_{\ell m}^*)$, $1 \leq \ell \leq r$, $0 \leq m \leq c_1(q^2 d)$ is a solution of a system of inhomogeneous linear equations over $k[X_1, \dots, X_{n-1}]$ with $\leq c_1(q^2 d) + qd \leq c_2(q^2 d)$ equations.

The coefficients of this system of equations are the $F_{k\ell m}^* \in R[X_1, \dots, X_{n-1}]$ with $\deg F_{k\ell m}^* = qd$, whereas the $Y_{\ell m}^*$ are in $k[X_1, \dots, X_{n-1}]$.

By recursion on n we conclude that there exists a function $f: \mathbb{N}^3 \rightarrow [0, \infty)$ such that to any $q \times r$ -system of inhomogeneous linear equations $M = (F_{k\ell})$ over $R[X_1, \dots, X_n]$ with $\sigma(M) \leq d$, solvable in $k[X_1, \dots, X_n]^r$, there exists a solution $(Z_1, \dots, Z_r) \in k[X_1, \dots, X_n]^r$ with $\deg Z_\ell \leq f(q, d, n)$, $1 \leq \ell \leq r$, and such that f has the following recursion property:

$$f(q, d, 0) = 0 \quad \text{and}$$

$$\text{for } n > 0 \quad f(q, d, n) \leq f(c_2(q^2 d), qd, n-1) + c_1(q^2 d).$$

Now the proof is complete.

Corollary 6: Let notations be as before. Let $F_1, \dots, F_S \in R[X_1, \dots, X_n]$ and $(F_1, \dots, F_S)$ be the ideal generated by $F_1, \dots, F_S$ in $K[X_1, \dots, X_n]$.

Then

$$1 \in (F_1, \dots, F_S) \quad \text{can be decided in } \sigma 2^{C(n+1) \log(n+1)} \text{ steps}$$

on a Turing-Machine, where $\sigma = \sum_{1 \leq k \leq S} \sigma(F_k)$.

Proof: By Lemma 8, $1 \in (F_1, \dots, F_S)$ iff there are $H_1, \dots, H_S \in K[X_1, \dots, X_n]$ with $\deg H_k \leq (c\sigma)3^n$ and $1 = \sum_{1 \leq k \leq S} H_k F_k$.

Comparing coefficients, this can be reduced to decide whether some

$(c\sigma)^n 3^n \times (c\sigma)^n 3^n$ -system of inhomogeneous linear equations M over R with $\sigma(M) = \sigma$ can be solved.

By Corollary 5 this needs $\leq \sigma 2^{C(n+1) \log(n+1)}$ steps on a Turing-Machine.

Corollary 7: Let notations be as before. Let k be an algebraically closed field containing R . The question whether

$$F_1 = 0 \wedge \dots \wedge F_r = 0 \wedge F_{r+1} \neq 0 \wedge \dots \wedge F_s \neq 0$$

defines a $F_1, \dots, F_s$ - cell, i.e. whether

$$\{x \in k^n; F_1(x) = 0, \dots, F_r(x) = 0, F_{r+1}(x) \neq 0, \dots, F_s(x) \neq 0\} \neq \emptyset$$

can be decided in $\sigma^{2^{c(n+1)} \log(n+1)}$ steps on a Turing - Machine.

Proof: Let T be a new indeterminate and put $F := F_{r+1} \cdot \dots \cdot F_s$.

By Hilbert's Nullstellensatz we have

$$\{x \in k^n; F_1 = 0, \dots, F_r = 0, F_{r+1} \neq 0, \dots, F_s \neq 0\} = \emptyset$$

$$\text{iff } 1 \in (F_1, \dots, F_s, 1 - TF) .$$

But by Corollary 6 this can be decided in $\sigma^{2^{c(n+1)} \log(n+1)}$ steps on a Turing - Machine.

Proposition 6: Let R be one of the rings $\mathbb{Z}, \mathbb{Z}_2, \dots, \mathbb{Z}_p, \dots$, where p is any prime number, and let k be an algebraically closed field containing R . Let $X_1, \dots, X_n$ be indeterminates over R and $F_1, \dots, F_s \in R[X_1, \dots, X_n]$. Then the conjunctions

$$F_{i_1} = 0 \wedge \dots \wedge F_{i_r} = 0 \wedge F_{i_{r+1}} \neq 0 \wedge \dots \wedge F_{i_s} \neq 0$$

defining $F_1, \dots, F_s$ - cells, i.e. non-empty sets in k^n , can be enumerated in $\sigma^{2^{c(n+1)} \log(n+1)}$ steps on a Turing - Machine, where $\sigma := \sum_{1 \leq k \leq s} \sigma(F_k)$.

Proof: The enumerating algorithm is defined recursively in $F_1, \dots, F_k, 1 \leq k \leq s$.

For $k=1$ we have to test whether $\{F_1 = 0\}$ is $\emptyset, k^n$ or different from both. In the first case, the expression $F_1 \neq 0$, and in the second case the expression $F_1 = 0$ define the unique F_1 - cells.^a In the third case, the F_1 - cells are defined by the expressions $F_1 = 0$ and $F_1 \neq 0$.

Let ϕ be a conjunction defining a $F_1, \dots, F_k$ - cell. Test whether $\phi \wedge F_{k+1} = 0$ defines $\emptyset, k^n$ or a set different from both.

In the first case only $\phi \wedge F_{k+1} \neq 0$ and in the second case only $\phi \wedge F_{k+1} = 0$ define $F_1, \dots, F_{k+1}$ - cells. In the third case $\phi \wedge F_{k+1} \neq 0$ and $\phi \wedge F_{k+1} = 0$ define $F_1, \dots, F_{k+1}$ - cells. In this way, starting from an enumeration of the conjunctions defining $F_1, \dots, F_k$ - cells, we get an enumeration of the conjunctions defining $F_1, \dots, F_{k+1}$ - cells.

After σ^{n+1} steps we stop the enumeration.

Since $1 + \sum_{1 \leq k \leq s} \deg F_k \leq \sigma$, we conclude from Corollary 1 that all conjunctions defining $F_1, \dots, F_s$ -cells are then enumerated. By Corollary 7 each test in the algorithm can be performed in time $\sigma^2 c_1(n+1) \log(n+1)$ on a Turing-Machine. So the whole recursive procedure can be performed in time $\sigma^2 c(n+1) \log(n+1)$.

Lemma 9: Let k be any field containing R . Let $M = (F_{kl})$, $F_{kl} \in R[X_1, \dots, X_n]$, a $q \times r$ -system of inhomogeneous linear equations. Then there exist polynomials $G_1, \dots, G_t \in R[X_1, \dots, X_n]$ such that

$$D := \{x \in k^n; (F_{kl}(x)) \text{ is solvable}\}$$

is a union of subsets of k^n defined by conjunctions $\phi_1, \dots, \phi_s$ of expressions of the form $G_1 = 0, \dots, G_t = 0$ and $G_1 \neq 0, \dots, G_t \neq 0$.

$G_1, \dots, G_t$ can be computed and $\phi_1, \dots, \phi_s$ can be enumerated in

$$(24) \quad r^2 (q \sigma(M))^{c(n+1)^2} \text{ steps on a Turing-Machine.}$$

Furthermore, we have

$$(25) \quad \sigma(G_i) \leq c(n+1)^2 q^3 \sigma(M), \quad 1 \leq i \leq t, \quad \text{and}$$

$$(26) \quad t \leq c r q^2 (q^2 \sigma(M))^n.$$

Proof: Recursively we construct the following items: A sequence $\phi_1, \dots, \phi_s$ of conjunctions built up by polynomials obtained from applying various Gauss-algorithms on M and a sequence $P_1, \dots, P_{s-1} \in R[X_1, \dots, X_n]$ of products of polynomials obtained in the same way.

To each $\phi_1, \dots, \phi_s$ there corresponds a Gauss-algorithm applied on M .

The $P_1, \dots, P_{s-1}$ are linearly independent over K , the field of fractions of R .

Let $\phi_1, \dots, \phi_i$ and $P_1, \dots, P_i$ be constructed. If all F_{kl} , $l \leq r$, are linearly dependent on $P_1, \dots, P_i$, we let the algorithm stop putting $s = i+1$ and

$$\phi_s := P_1 = 0 \wedge \dots \wedge P_{s-1} = 0 \wedge F_{1r+1} = 0 \wedge \dots \wedge F_{qr+1} = 0$$

If not, we choose any $F_{k\ell}$, $\ell \leq r$, linearly independent on $P_1, \dots, P_i$ as the first pivot of a Gauss-algorithm on M .

We put

$$P_{i+1}^{(1)} := F_{k\ell}$$

$$\text{and } \phi_{i+1}^{(1)} := P_{i+1}^{(1)} \neq 0 \wedge P_1 = 0 \wedge \dots \wedge P_i = 0 \wedge \bigwedge_{\substack{F_{k1}, \dots, F_{kr} \\ \text{lin. dep. on} \\ P_1, \dots, P_i}} F_{kr+1} = 0$$

After j such steps, $1 \leq j < q$, we arrive at the following situation:

we have constructed a Gauss-algorithm $M = M_1, \dots, M_j = (F_{k\ell}^{(j)})$,

polynomials $P_{i+1}^{(1)}, \dots, P_{i+1}^{(j)}$, and a conjunction $\phi_{i+1}^{(j)}$.

If all $F_{k\ell}^{(j)} \cdot P_{i+1}^{(j)}$, $\ell \leq r$, $j < k$, are linearly dependent on $P_1, \dots, P_i$, we put

$$P_{i+1} := P_{i+1}^{(j)}$$

$$\text{and } \phi_{i+1} := \phi_{i+1}^{(j)}.$$

If not, we choose any $F_{k\ell}^{(j)}$, $\ell \leq r$, $j < k$, such that $F_{k\ell}^{(j)} \cdot P_{i+1}^{(j)}$ is linearly independent on $P_1, \dots, P_i$ as the $(j+1)$ -st pivot of the Gauss-algorithm and continue the Gauss-algorithm by one step.

We put

$$P_{i+1}^{(j+1)} := F_{k\ell}^{(j)} \cdot P_{i+1}^{(j)}$$

$$\text{and } \phi_{i+1}^{(j+1)} := \phi_{i+1}^{(j)} \wedge P_{i+1}^{(j+1)} \neq 0 \wedge \bigwedge_{\substack{F_{k1}^{(j)} \cdot P_{i+1}^{(j)}, \dots, F_{kr}^{(j)} \cdot P_{i+1}^{(j)} \\ \text{lin. dep. on } P_1, \dots, P_i}} F_{kr+1}^{(j)} = 0.$$

In the case $j = q$, we put

$$P_{i+1} := P_{i+1}^{(j)}$$

$$\phi_{i+1} := \phi_{i+1}^{(j)}.$$

Since any polynomial linearly dependent on $P_1, \dots, P_i$ vanishes on $\{P_1 = 0, \dots, P_i = 0\}$, the reader easily verifies:

- (i) For $x \in k^n$ with $P_1(x) = 0, \dots, P_{i-1}(x) = 0, P_i(x) \neq 0$
 $M(x) := (F_{k\ell}(x))$ is solvable iff x is in the set D_i defined by ϕ_i in k^n .
- (ii) For $x \in k^n$ with $P_1(x) = 0, \dots, P_{s-1}(x) = 0$ $M(x)$ is solvable iff $x \in D_s$.

Hence, by (i) and (ii)

$$D := \{x \in k^n; M(x) \text{ is solvable}\} = \bigcup_{1 \leq i \leq s} D_i.$$

Let $G_1, \dots, G_t$ be the polynomials appearing in $\phi_1, \dots, \phi_s$.

By Remark 6 and (10) we have $\sigma(G_i) \leq c(n+1)^2 q^3 \sigma(M)$, $1 \leq i \leq t$, whence (25).

Furthermore, by Remark 6 and (13), $G_1, \dots, G_t$ can be computed in $s r (q \sigma(M))^{c_1(n+1)}$ steps on a Turing-Machine.

For the enumerating of $\phi_1, \dots, \phi_s$ we have to check additionally linear independency over K of some of the $G_1, \dots, G_t$.

By comparison of coefficients, this checks can be reduced to test solvability of some inhomogeneous linear equation systems over R . By Corollary 5 this can be done in $(rs)^2 (q \sigma(M))^{c_2(n+1)^2}$ steps on a Turing-Machine.

So, computing $G_1, \dots, G_t$ and constructing $\phi_1, \dots, \phi_s$ together costs

$$(27) \quad (rs)^2 (q \sigma(M))^{c_3(n+1)^2} \text{ Turing-Machine steps.}$$

Furthermore, we have

$$(28) \quad t \leq c_4 r q^2 s.$$

The crucial point in the proof is the estimation of s , the number of steps of the algorithm.

Note that $P_1, \dots, P_{s-1}$ are linearly independent polynomials from $K[X_1, \dots, X_n]$ all of degree $< q^2 \sigma(M)$. Hence $s \leq (q^2 \sigma(M))^n + 1$.

Together with (27) and (28) this gives (24) and (26).

We shall apply Lemma 9 only to algebraically closed fields k .

Proposition 7: Let R be one of the rings $\mathbb{Z}, \mathbb{Z}_2, \dots, \mathbb{Z}_p, \dots$, where p is any prime number, $X_1, \dots, X_n$ indeterminates over R , $F_1, \dots, F_s \in R[X_1, \dots, X_n]$ with $\sigma = \sum_{1 \leq i \leq s} \sigma(F_i)$, k an algebraically closed field containing R , and $0 \leq m \leq n$.

Then there exist $t \leq s^2 c^m \log(n+1)$ polynomials $G_1, \dots, G_t \in R[X_1, \dots, X_{n-m}]$

with $\sigma(G_i) \leq \sigma^2 c^m \log(m+1)$, $1 \leq i \leq t$, such that

$$D = \{x \in k^{n-m}; \exists x' \in k^m \quad F_1(x, x') = 0, \dots, F_r(x, x') = 0, F_{r+1}(x, x') \neq 0, \dots, F_s(x, x') \neq 0\}$$

is definable by a quantifier free formula Ψ which is built up by the prime formulas $G_1 = 0, \dots, G_t = 0$.

There is a Turing-Machine which computes $G_1, \dots, G_t$ and constructs Ψ in $\leq \sigma^2 c^m \log(n+1)$ steps.

Proof: We consider $E := k^{n-m} - D$.

Let T be a new indeterminate and $X' := (X_{n-m+1}, \dots, X_n)$.

Then $E = \{x \in k^{n-m}; F_1(x, X'), \dots, F_r(x, X'), 1 - T \cdot F_{r+1}(x, X') \cdot \dots \cdot F_s(x, X') \text{ have no common zero in } k^{m+1}\}$.

By Hilbert's Nullstellensatz and Lemma 8

$F_1(x, X'), \dots, F_r(x, X'), 1 - T \cdot F_{r+1}(x, X') \cdot \dots \cdot F_s(x, X')$ have no common zero

iff there exist $H_1(X', T), \dots, H_r(X', T), H(X', T) \in k[X', T]$ with

$$\deg H_1, \dots, \deg H_r, \deg H \leq (c\sigma)3^{m+1}$$

such that

$$1 = H_1(X', T) \cdot F_1(x, X') + \dots + H_r(X', T) \cdot F_r(x, X') + H(X', T)(1 - T \cdot F_{r+1}(x, X') \cdot \dots \cdot F_s(x, X'))$$

By comparing coefficients, the problem to decide whether such $H_1, \dots, H_r, H$ exist, can be reduced to decide the solvability of some

$(c\sigma)3^{(m+1)\log(m+1)} \times (c\sigma)3^{(m+1)\log(m+1)}$ - system of inhomogeneous linear

equations $M(x) := (F_{kl}(x))$, where the $F_{kl} \in R[X_1, \dots, X_{n-m}]$ are the coefficients of $F_1, \dots, F_r$ and $1 - T \cdot F_{r+1} \cdot \dots \cdot F_s$. ($F_1, \dots, F_r$ and $1 - T \cdot F_{r+1} \cdot \dots \cdot F_s$ are considered as polynomials in X' and T .)

So we have $E = \{x \in k^{n-m}; M(x) \text{ is solvable}\}$.

Applying the algorithm of Lemma 9 to $M := (F_{kl})$ we obtain polynomials

$G_1, \dots, G_t \in R[X_1, \dots, X_{n-m}]$ and conjunctions $\phi_1, \dots, \phi_s$ built up from $G_1, \dots, G_t$ such that E is a union of the subsets of k^{n-m} defined by $\phi_1, \dots, \phi_s$.

Thus D as the complement of E in k^{n-m} is defined by $\Psi := \neg \phi_1 \wedge \dots \wedge \neg \phi_s$.

The time and length bounds stated in Proposition 7 follow from the bounds in Lemma 9.

Theorem 6: Let R be one of the rings $\mathbb{Z}, \mathbb{Z}_2, \dots, \mathbb{Z}_p, \dots$, where p is any prime number. Let k be an algebraically closed field containing R .

Furthermore let $(Q_{n-m+1} X_{n-m+1}) \dots (Q_n X_n) \phi(X_1, \dots, X_n)$ be a first order formula in the language $(0, 1, +, \cdot, =)$ with quantifiers $Q_{n-m+1}, \dots, Q_n$ and with $\phi(X_1, \dots, X_n)$ quantifier-free. Let $\phi(X_1, \dots, X_n)$ be built up by prime formulas of the form $F_1 = 0, \dots, F_s = 0$, $F_1, \dots, F_s \in R[X_1, \dots, X_n]$, and let

$\sigma := \bigwedge_{1 \leq k \leq s} \sigma(F_k)$. Then a quantifier-free formula $\psi(X_1, \dots, X_{n-m})$ can be

constructed in time $\leq \sigma 2^{\sigma m(n+1) \log(n+1)}$, such that

$(Q_{n-m+1} X_{n-m+1}) \dots (Q_n X_n) \phi(X_1, \dots, X_n)$ and $\psi(X_1, \dots, X_{n-m})$ are equivalent, i.e. define the same subset of k^{n-m} .

Proof: We use standard techniques of quantifier elimination proofs.

By Proposition 6 and Proposition 7 we get the bounds stated in Theorem 6 .

As an illustration how these propositions come in, we consider the formula $(Q_n X_n) \phi(X_1, \dots, X_n)$ and eliminate $(Q_n X_n)$. We assume Q_n to be the universal quantifier $\forall$. (The case that Q_n is the existential quantifier $\exists$ can be treated analogously.)

First we substitute $(\forall X_n)$ in $(\forall X_n) \phi(X_1, \dots, X_n)$ by $\neg(\exists X_n) \neg$. By Proposition 6 we find conjunctions $F_{i_1} = 0 \wedge \dots \wedge F_{i_r} = 0 \wedge F_{i_{r+1}} \neq 0 \wedge \dots \wedge F_{i_s} \neq 0$ such that $\neg \phi$ is equivalent to the disjunction of them.

Then we substitute $(\exists X_n) \neg \phi(X_1, \dots, X_n)$ by the disjunction of the formulas

$$\begin{aligned} (\exists X_n) \quad & F_{i_1}(X_1, \dots, X_n) = 0 \wedge \dots \wedge F_{i_r}(X_1, \dots, X_n) = 0 \wedge \\ & \wedge F_{i_{r+1}}(X_1, \dots, X_n) \neq 0 \wedge \dots \wedge F_{i_s}(X_1, \dots, X_n) \neq 0 \end{aligned}$$

and eliminate in each of these formulas $(\exists X_n)$ by means of Proposition 7.

In this way we get polynomials $G_1, \dots, G_t \in k[X_1, \dots, X_{n-1}]$ such that $(\exists X_n) \neg \phi(X_1, \dots, X_n)$ is equivalent to some Boolean combination ψ of $G_1 = 0, \dots, G_t = 0$.

Once more, by Proposition 6, $\neg \psi$, which is equivalent to $(\forall X_n) \phi(X_1, \dots, X_n)$, can be written as some disjunction of expressions defining $G_1, \dots, G_t$ -cells.

References

- Atiyah, M.F. & Macdonald, I.G. : Introduction to Commutative Algebra.
(Addison-Wesley, Reading Mass., 1969).
- Bareiss, E.H. : Sylvester's Identity and Multistep Integer Preserving Gaussian Elimination. Math. Comp. 22, 103 (1968) 565-578.
- Baur, W. & Strassen, V. : The complexity of partial derivatives. 1981
(to appear in Theoret. Comput. Sci.).
- Collins, G.E. : Quantifier elimination for real closed fields by cylindrical algebraic decomposition.
LN Comput. Sci. 33 (Springer, Berlin, 1975) 134-183.
- Edmonds, J. : Systems of Distinct Representatives and Linear Algebra.
J. of Research of the National Bureau of Standards 71B, 4
(1967) 241-245.
- Fischer, M.J. & Rabin, M.D. : Super-Exponential Complexity of Presburger Arithmetic. MAC Technical Memorandum 43 (M.I.T., 1974).
- Heintz, J. & Wüthrich, R. : An efficient quantifier elimination algorithm for algebraically closed fields of any characteristic.
SIGSAM Bulletin 9, Nr. 4 (November 1975) 11.
- Heintz, J. : Definability bounds in algebraically closed fields and a note on degree in affine algebraic geometry. 1977 (preprint).
Presented at the 1977 Oberwolfach Conference on Complexity Theory.
- Heintz, J. : Definability bounds of first order theories of algebraically closed fields.
Extended abstract in: Fundamentals of Computation Theory FCT'79.
Ed. by L. Budach (Akademie-Verlag, Berlin, 1979) 160-166.
- Heintz, J. & Schnorr, C.P. : Testing Polynomials which are Easy to compute.
12th Annual Symp. ACM on Computing (1980) 262-272.
- Heintz, J. & Sieveking, M. : Lower bounds for polynomials with algebraic coefficients. Theoret. Comput. Sci. 11 (1980) 321-330.
- Heintz, J. & Sieveking, M. : Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables.
in: Automata, Languages and Programming. Eighth Colloquium Acre (Akko) Israel, July 1981. Ed. by S. Even and O. Kariv.
LN Comput. Sci. 115 (Springer, Berlin, 1981) 16-28.
- Hermann, G. : Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. 95 (1926) 736-788.
- Iversen, B. : Generic local structure of the morphisms in commutative algebra. LN Math. 310 (Springer, Berlin, 1973).
- Lang, S. : Algebra. (Addison-Wesley, Reading Mass., 1969).
- Lang, S. : Introduction to Algebraic Geometry. 3rd printing.
(Addison-Wesley, Reading Mass., 1972).

- Monck, L. : An Elementary - Recursive Decision Procedure for $\text{Th}(\mathbb{R}, +, \cdot)$.
Univ. of Calif., Berkeley, Dept. of Math. 1974 (preprint).
- Mumford, D. : Introduction to Algebraic Geometry.
Harvard University (mimeographed notes).
- Samuel, P. : Méthodes d'algèbre abstraite en géométrie algébrique. 2nd ed.
(Springer, Berlin, 1967).
- Schnorr, C.P. : An extension of Strassen's degree bound.
SIAM J. on Comput. 10 (1981) 371-382.
- Seidenberg, A. : Constructions in Algebra.
Trans. Amer. Math. Soc. 197 (1974) 273-313.
- Shafarevich, I.R. : Basic algebraic geometry.
(Nauka, Moscow, 1972); in English: (Springer, Berlin, 1974).
- Solovay, R. : Private communication, 1975.
- Strassen, V. : Die Berechnungskomplexität von elementarsymmetrischen
Funktionen und von Interpolationskoeffizienten.
Numer. Math. 20 (1973) 238-251.
- Strassen, V. : The Computational Complexity of Continued Fractions.
Proc. of the 1981 ACM Symp. on Symbolic and Algebraic
Computation (1981) 51-67.
- van der Waerden, B.L. : Algebra I. 8. Auflage der Modernen Algebra. HT Bd. 12
(Springer, Berlin, 1971).
- Wüthrich, H.R. : Ein Entscheidungsverfahren für die Theorie der reell-
abgeschlossenen Körper.
in: E. Specker & V. Strassen : Komplexität von Entscheidungs-
problemen. Ein Seminar.
IN Comput. Sci. 43 (Springer, Berlin, 1976) 138-162.
- Wüthrich, H.R. : Ein schnelles Quantoreneliminationsverfahren für die Theorie
der algebraisch abgeschlossenen Körper.
Ph. D. thesis, Univ. of Zurich, 1977.

Lebenslauf

27. 10. 1945 in Zürich geboren. Bürger von Davos GR
- 1965 Matura des Typus A (klassisches Gymnasium) in Wetzikon bei Zürich
- 1965 Studium der Philosophie an der Universität Zürich
- 1968 - 1972 Assistent am Seminar für Angewandte Mathematik der Universität Zürich
- 1972 Diplom in Mathematik an der Universität Zürich
- Winter 1972/73 Aufenthalt an der Prirodnoslovno - Matematički Fakultet der Universität Zagreb
- 1973 - 1976 Assistent am Seminar für Angewandte Mathematik der Universität Zürich
- 1977 verschiedene Berufstätigkeiten ausserhalb der Mathematik
- 1978 - 1982 Wissenschaftlicher Mitarbeiter im Fachbereich Mathematik der J.W. v. Goethe - Universität in Frankfurt/M

In Zürich besuchte ich Vorlesungen und Seminare bei den Herren Professoren Eckmann, Gabriel, Gross, Karrer, Läuchli, Specker, Strassen, van der Waerden.

